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

Mannheim, den 6. Februar 2026

Sozialgericht Berlin
Invalidenstr. 52
10557 Berlin

In dem Verfahren

Kurz ./. [redacted]

– S 220 SF 13/22 DS –

ist das Verfahren weiterzuführen, da das Forschungsdatenzentrum Gesundheit am 9. Oktober 2025 seinen operativen Betrieb aufgenommen hat.

In der Zwischenzeit haben sich die Rechtsgrundlagen des Forschungsdatenzentrums geändert. In §§ 303a ff. SGB V wurden insbesondere die Frequenz der Datenübermittlung von einer jährlichen auf eine quartalsweise Übermittlung erhöht, die Dauer der Datenspeicherung von 30 auf 100 Jahre verlängert, weitere Nutzungszwecke für die gespeicherten Daten eingeführt und der Kreis der nutzungsberechtigten Stellen erheblich erweitert. Zudem wurde die DaTraV aufgehoben und in eine allgemeine Verordnung zur Regelung der Verfahren beim Forschungsdatenzentrum Gesundheit (FDZGesV) überführt, die neben dem Datentransparenzverfahren nach §§ 303a ff. SGB V auch Einzelheiten der Verarbeitung von Daten der elektronischen Patientenakte zu Forschungszwecken nach § 363 SGB V regelt. Inhaltlich haben sich hierbei keine größeren Veränderungen ergeben. Schließlich können die Daten aus dem Datentransparenzverfahren nunmehr gemäß § 4 GDNG mit Daten der klinischen Krebsregister der Länder verknüpft werden. Insgesamt helfen die neuen Re-

gelungen den im vorliegenden Verfahren erhobenen Rügen gegen das Datentransparenzverfahren nicht ab. Teilweise vertiefen sie die Defizite der Rechtsgrundlagen dieses Verfahrens sogar noch.

Im Einzelnen habe ich diese Defizite in meinem Schriftsatz vom 1. Februar 2023 aufgrund des damaligen Verfahrensstands nochmals gebündelt und vertieft erörtert. Im Folgenden beschränke ich mich auf eine geraffte Darstellung, die sich an diesem Schriftsatz orientiert, allerdings die geänderte Rechtslage sowie die mir nach dem 1. Februar 2023 zugegangenen Schriftsätze der Beigeladenen zu 1 und zu 4 und die in der zweiten mündlichen Verhandlung vorgebrachten Argumente einbezieht.

Danach ist daran festzuhalten, dass die Zentralisierung der Datenhaltung bei dem Forschungsdatenzentrum erhebliche Risiken und Nachteile mit sich bringt, die nicht aufgrund von Funktionalitätsvorteilen hingenommen werden können (unten I.). Das Datentransparenzverfahren weist zudem weitere Sicherheitsmängel auf (unten II.). Schließlich muss den betroffenen Personen jedenfalls bei der gegenwärtigen Ausgestaltung der Datenverarbeitung ein voraussetzungsloses Widerspruchsrecht gegen die Übermittlung der auf sie bezogenen Daten an die Datensammelstelle eingeräumt werden (unten III.).

I. Zentralisierung der Datenhaltung im Forschungsdatenzentrum

In meinem Schriftsatz vom 1. Februar 2023 habe ich zur Zentralisierung der Datenhaltung ausgeführt, dass diese ein vermeidbares zusätzliches Sicherheitsrisiko schafft. Zudem ermöglicht nur eine dezentrale Datenhaltung umfassend, bei der Nutzung der gespeicherten Daten Vorkehrungen zum Schutz der betroffenen Personen wie lokale *Differential Privacy* oder sichere verteilte Berechnungen zu implementieren. Demgegenüber verursacht eine dezentrale Datenhaltung keine erheblichen Funktionalitätseinbußen, deretwegen die Nachteile einer zentralen Datenhaltung hingenommen werden könnten. An diesen Befunden hat sich in der Zwischenzeit nichts geändert.

1. Zentrale Datenhaltung als zusätzliches Sicherheitsrisiko

Die gesetzlich vorgegebene zentrale Datenhaltung bei der Beigeladenen zu 4 führt dazu, dass ein weiterer angreifbarer Bestand von hoch sensiblen Gesundheitsdaten geschaffen wird, der zu den dezentralen Datenbeständen der Krankenkassen hinzutritt. Hierin liegt unabhängig davon, mit welchen Mitteln der zentrale Datenbestand gesichert wird, ein zusätzliches Sicherheitsrisiko, da sich eine vollständige Datensicherheit nie gewährleisten lässt.

Hierbei handelt es sich nicht um ein theoretisches Problem. Vielmehr ist mit hoher Wahrscheinlichkeit davon auszugehen, dass es zu erfolgreichen Angriffen auf den Datenbestand des Forschungsdatenzentrums kommen wird. Solche Angriffe sind ein alltägliches Phänomen, dem auch technisch-organisatorisch hoch kompetente Datenverarbeiter ausgesetzt sind.

Zur Veranschaulichung der schieren Masse von Datenabflüssen, gerade auch von Gesundheitsdaten im Bestand öffentlicher Stellen, kann beispielhaft auf die Zusammenstellung der US-amerikanischen Organisation Privacy Rights Clearinghouse verwiesen werden, die Informationen über öffentlich bekanntgemachte Datenabflüsse US-amerikanischer öffentlicher Stellen zusammenträgt. Diese bis zum Jahr 2005 zurückreichende Zusammenstellung umfasst derzeit mehr als 75.000 Bekanntmachungen, von denen sich über 15.000 auf Datenbestände aus dem Bereich der Gesundheitsversorgung beziehen,

vgl. https://privacyrights.org/data-breaches.

Kommt es zu einem Abfluss pseudonymisierter Daten aus dem Datenbestand des Forschungsdatenzentrums, so ist zudem wahrscheinlich, dass sich diese Daten zum Nachteil betroffener Personen verwenden lassen, indem diese Personen reidentifiziert werden.

Für eine solche Reidentifikation werden die abgeflossenen Forschungsdaten mit weiteren Datenbeständen verknüpft. Bereits wenige zusätzliche Informationen können ausreichen, um ein hohes Reidentifikationsrisiko zu begründen. Ein berühmter Beispielsfall stammt aus dem Jahr 1997: Eine Forscherin konnte durch die Verknüpfung eines für Forschungszwecke verfügbaren anonymisierten medizinischen Datenbestands mit öffentlich verfügbaren Wählerregisterdaten der Stadt Cambridge (Massachusetts) den damaligen Gouverneur von Massachusetts in dem medizinischen Datenbestand identifizieren. Für den erfolgreichen Abgleich genügten drei übereinstimmende Merkmale (Geburtsdatum, Geschlecht, Postleitzahl),

vgl. für eine Darstellung des Falls und der Vorgehensweise Ohm, UCLA Law Review 57 (2010), 1701 (1719 f.); den empirischen Hintergrund erläutert Sweeney, Simple Demographics Often Identify People Uniquely, 2000, https://dataprivacylab.org/projects/identifiability/paper1.pdf; die Aussagekraft dieses Falls relativiert, ohne das grundsätzliche Reidentifikationsrisiko zu bestreiten, Barth-Jones, The „Re-identification“ of Governor William Weld’s Medical Information, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397.

Heute sind aufgrund der informationstechnischen und sozialen Entwicklung sowohl viel mehr für eine Reidentifikation nutzbare öffentlich zugängliche Daten als auch weitaus fortgeschrittenere Analysemethoden verfügbar als 1997. Es ist davon auszugehen, dass sich ein Datenbestand wie der des Forschungsdatenzentrums zu einem erheblichen Teil mit Hilfe solcher Daten und Methoden zuordnen lässt,

> vgl. zu dem – großen – Reidentifikationspotenzial von Krankenkassenabrechnungsdaten Drechsler/Pauly, Bundesgesundheitsblatt 2024, S. 164 (165 f.).

Hingegen kann die von der Beigeladenen zu 4 mit Schriftsatz vom 3. Februar 2023 vorgelegte gutachterliche Stellungnahme verschiedener medizinisch-wissenschaftlicher Experten (im Folgenden: Stellungnahme), die eine Reidentifikation für unrealistisch hält, nicht überzeugen. Hierfür gibt es vor allem zwei Gründe:

Erstens befasst sich die Stellungnahme nur mit einer Reidentifikation durch die zugelassenen Nutzer des Forschungsdatenzentrums. Die Sicherheitsbedenken gegen die Zentralisierung der Datenhaltung ergeben sich hingegen maßgeblich auch aus dem Risiko einer Reidentifikation durch externe Angreifer, die auf den Datenbestand des Forschungsdatenzentrums zugegriffen haben. Gegenüber solchen Angreifern helfen die rechtlichen, organisatorischen und technischen Vorkehrungen, die für Datenverarbeitungen im Rahmen der zugelassenen Nutzung gelten und auf die sich die Stellungnahme bezieht, naturgemäß nicht. Die Stellungnahme liegt darum in diesem Punkt bereits hinsichtlich ihres Gegenstands teils neben der Sache.

Zweitens bezeichnet die Stellungnahme als Reidentifikation nur den Fall einer „eindeutigen Reidentifikation“, in dem ein bestimmter Datensatz mit Sicherheit einer bestimmten Person zugeordnet werden kann. Jedoch kann auch eine lediglich mit einer gewissen Wahrscheinlichkeit gelungene Reidentifikation die Interessen der betroffenen Personen erheblich gefährden. Gelingt Kriminellen eine solche (lediglich) wahrscheinliche Reidentifikation, so können sie die erlangten Gesundheitsdaten beispielsweise zu Erpressungsversuchen nutzen. Dass ein solcher Versuch ins Leere gehen mag, wenn die Person, der die Daten zugeordnet wurden, tatsächlich nicht die betroffene Person ist, ändert nichts daran, dass die durch korrekte Zuordnungen betroffenen Personen hierdurch erhebliche Schäden erleiden können. Das kriminelle „Geschäftsmodell“ geht bereits auf, wenn nur ein kleiner Bruchteil der Erpressungsversuche erfolgreich ist.

2. Vorteile der dezentralen Datenhaltung

Eine dezentrale Datenhaltung bei den Krankenkassen würde nicht nur die Sicherheitsmängel der zentralen Datenhaltung vermeiden, sondern zudem ermöglichen, die Rechte der betroffenen Personen vollumfänglich wahrzunehmen und Verfahren zum Schutz der betroffenen Personen bei der Datennutzung umfassend zu implementieren. In meinem Schriftsatz vom 1. Februar 2023 habe ich letzteren Punkt für die lokale Variante von *Differential Privacy* und für verteilte Berechnungen näher ausgeführt.

Soweit die Stellungnahme den Nutzen von *Differential Privacy* und einer dezentralen Datenauswertung für die medizinische Forschung bestreitet, überzeugt dies nicht. Die Stellungnahme verkennt sowohl die Argumentation der Klägerin als auch die Funktionsweise dieser Verfahren.

Die Klägerin hat nie vorgetragen, dass die von ihr genannten Schutzvorkehrungen in jedem einzelnen Auswertungsprojekt genutzt werden sollen. Vielmehr habe ich in meinem Schriftsatz vom 1. Februar 2023 näher ausgeführt, dass es hierfür auf eine Abwägung zwischen konfligierenden Interessen (etwa einem möglichst wirksamen Datenschutz einerseits, einer möglichst exakten oder zeitnahen Datenauswertung andererseits) ankommen kann, die je nach Auswertungsprojekt unterschiedlich ausgehen kann. Nur die dezentrale Datenhaltung ermöglicht jedoch eine umfassende Abwägung, während die zentrale Datenhaltung bestimmte Schutzoptionen von vornherein abschneidet. Anders als die Stellungnahme suggeriert, handelt es sich hierbei um Optionen, die praktisch in vielen Fällen in Betracht kommen.

Mit Blick auf *Differential Privacy* geht die Stellungnahme teils von verzerrten Prämissen aus. Anders als die Schlussfolgerung der Stellungnahme suggeriert, geht es hierbei nicht darum, den Forschungsdatenbestand im Voraus generell zu verrauschen, was ihn in der Tat für viele Auswertungsprojekte unbrauchbar machen dürfte. Beim Einsatz von *Differential Privacy* werden vielmehr erst die Ergebnisse konkreter Berechnungen im Rahmen einzelner Projekte verrauscht, sodass aus diesen Ergebnissen nicht auf die einzelnen betroffenen Personen geschlossen werden kann. Dieses Verrauschen erfolgt zudem nicht arbiträr, sondern nach Maßgabe bestimmter mathematischer Parameter, gerade um ein brauchbares Ergebnis sicherzustellen.

Es mag zutreffen, dass sich *Differential Privacy* weder in der lokalen noch in der zentralen Variante für alle Auswertungsprojekte eignet. Maßgeblich für die Argumentation der Klägerin ist jedoch, dass dieses Verfahren gerade auch in der lokalen Variante eine Option für bestimmte Projekte sein kann, die durch

die Zentralisierung des Datenbestands von vornherein abgeschnitten wird. Dies ist auch etwa der Tenor der in der Stellungnahme zitierten Beiträge von *Boenisch*, die in den zitierten Passagen *Differential Privacy* keineswegs generell als ungeeignet bezeichnet, sondern – zutreffend – von einem „Trade-Off zwischen Nutzbarkeit der Analysen und Privatsphäre der Daten, welcher problemspezifisch abgewogen werden muss“, spricht.

Unzutreffend ist die Behauptung der Stellungnahme, *Differential Privacy* sei für kategoriale Variablen ungeeignet. Viele Arbeiten über die lokale Variante von *Differential Privacy* wurden vielmehr gerade für solche Daten entwickelt,

> grundlegend waren etwa die viel zitierten Beiträge von McSherry/Talwar, Mechanism Design via Differential Privacy, Foundations of Computer Science 2007, 94; Erlingsson/Pihur/Korolova, RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response, ACM CCS 2014, 1054, https://share.google/XGudUJVlEIXCTeRUm.

Diese Arbeiten enthalten formale mathematische Beweise dafür, dass das Ergebnis der Berechnung nahe an dem unverrauschten Ergebnis ist, sodass dysfunktionale Kategorienfehler vermieden werden.

Insbesondere zum Einsatz von *Differential Privacy* für die medizinische Forschung gibt es zahlreiche Arbeiten, die die grundsätzliche Tauglichkeit dieses Verfahrens belegen,

> vgl. etwa Mohammed u.a., Privacy-preserving heterogeneous health data sharing, J Am Med Inform Assoc. 2013 May 1;20(3):462-9, doi: 10.1136/amiajnl-2012-001027; Sung/Cha/Park, Local Differential Privacy in the Medical Domain to Protect Sensitive Information: Algorithm Development and Real-World Validation, JMIR Med Inform. 2021 Nov 8;9(11):e26914, doi: 10.2196/26914; Dyda u.a., Differential privacy for public health data: An innovative tool to optimize information sharing while protecting data confidentiality, Patterns (N Y), 2021 Dec 10;2(12):100366, doi: 10.1016/j.patter.2021.100366.

Soweit die Stellungnahme eine dezentrale Datenauswertung für die medizinische Forschung für untauglich hält, geht sie an den Ausführungen der Klägerin vorbei. Die Stellungnahme impliziert, dass Berechnungen lokal durchgeführt und die Ergebnisse im Anschluss zusammengeführt werden. Dies ist jedoch nicht die Funktionsweise der in meinem Schriftsatz vom 1. Februar 2023 dargestellten verteilten sicheren Berechnung. Bei diesem Verfahren wird vielmehr

ebenso wie bei einer zentralen Berechnung nur eine Berechnung durchgeführt, an der jedoch mehrere Stellen teilnehmen. Das Ergebnis bleibt dementsprechend dasselbe wie bei einer zentralen Berechnung. Wie bereits in den 1980er Jahren gezeigt wurde, kann mit entsprechender Rechenkapazität *jede* Berechnung sicher verteilt realisiert werden. Auch insoweit verweise ich auf meinen Schriftsatz vom 1. Februar 2023.

Ob beim gegenwärtigen Stand der Technik alle Forschungsprojekte, die im Rahmen des Forschungsdatenzentrums anfallen, bei vertretbarem Ressourceneinsatz mit sicheren verteilten Berechnungen durchgeführt werden könnten, bedarf im vorliegenden Verfahren keiner Entscheidung. Jedenfalls handelt es sich um einen leistungsfähigen Ansatz, der für viele Projekte in Betracht kommt und ein hohes Datenschutzniveau gewährleisten kann. Die Zentralisierung der Datenhaltung schneidet diese Option von vornherein ab.

Das in der Stellungnahme erörterte föderierte Lernen ist hingegen eine völlig andere Auswertungsmethode als verteilte Berechnungen, die eigene Stärken und Schwächen aufweist. Die Stellungnahme geht daher mit Blick auf die dezentrale Datenauswertung an den Ausführungen der Klägerin vorbei. Allerdings kann je nach Auswertungsprojekt föderiertes Lernen eine funktionale Datenauswertung ermöglichen und zugleich die Belange der betroffenen Personen wahren. Auch der je nach Fallgestaltung denkbare Einsatz dieses Verfahrens wird durch die Zentralisierung des Datenbestands vereitelt,

> vgl. zur Funktionsweise verteilter maschineller Lernverfahren The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics, 2023, https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf, S. 43 ff.

3. Keine übermäßigen Funktionalitätseinbußen bei dezentraler Datenhaltung

Eine dezentrale Datenhaltung ermöglicht insgesamt eine leistungsfähige Datenauswertung, die zugleich die Defizite der zentralen Datenhaltung vermeidet. Insoweit verweise ich wiederum auf meinen Schriftsatz vom 1. Februar 2023.

II. Weitere Sicherheitsmängel des Datentransparenzverfahrens

Über die Zentralisierung der Datenhaltung hinaus weist das Datentransparenzverfahren in seiner gegenwärtigen Ausgestaltung weitere Sicherheitsmängel auf, die zumindest in einer Gesamtschau zur Unanwendbarkeit der §§ 303a ff. SGB V führen.

Wie in meinem Schriftsatz vom 1. Februar 2023 ausgeführt, ist nicht nachvollziehbar, warum neben der Datenhaltung auch der Datentransfer zentralisiert wird. Dies hat zur Folge, dass bei der Datensammelstelle ein weiterer angreifbarer Datenbestand entsteht. Dieses Defizit des Datentransparenzverfahrens hat sich durch die jüngsten Rechtsänderungen noch verschärft, da gemäß § 303a Abs. 1 SGB V nunmehr quartalsweise jeweils die Daten eines ganzen Jahres zu übermitteln sind. Dadurch wird der Datenbestand bei der Datensammelstelle häufiger angelegt und kann dementsprechend häufiger angegriffen werden.

Auch die Regelungen über die Datennutzung sind nach wie vor unzureichend. Der heutige Rechtsrahmen verschärft die Risiken der Datennutzung für die betroffenen Personen noch erheblich, da sich sowohl die zulässigen Nutzungszwecke als auch der Kreis der Nutzungsberechtigten stark erweitert haben.

Zulässig ist mittlerweile unter anderem eine Nutzung zur Entwicklung, Weiterentwicklung, Überwachung der Sicherheit und Nutzenbewertung von Arzneimitteln, Medizinprodukten, Untersuchungs- und Behandlungsmethoden, Hilfs- und Heilmitteln, digitalen Gesundheits- und Pflegeanwendungen sowie Systemen der Künstlichen Intelligenz im Gesundheitswesen (§ 303e Abs. 2 Nr. 9 und 10 SGB V). Nutzungsberechtigt sind zudem nicht mehr nur bestimmte (überwiegend öffentliche) Stellen, sondern beliebige natürliche und juristische Personen, soweit sie zulässige Nutzungszwecke verfolgen (§ 303e Abs. 1 Satz 2 SGB V). Damit haben sich die Risiken eines unbeabsichtigten Datenabflusses wie auch einer missbräuchlichen Datennutzung deutlich erhöht, wie sich auch an den nunmehr erforderlichen ausdrücklichen Nutzungsverboten in § 303e Abs. 3a Satz 2 SGB V zeigt.

Besonders große Risiken begründet die neu geschaffene Möglichkeit, den Datenbestand des Forschungsdatenzentrums für die Entwicklung von Systemen der Künstlichen Intelligenz im Gesundheitswesen zu nutzen. Insbesondere gilt dies für den Fall, dass die Daten zum Trainieren von KI-Systemen genutzt werden. Zum einen ist in diesem Fall damit zu rechnen, dass ein besonders großer Datenbestand in Form pseudonymisierter Einzeldatensätze bereitgestellt wird. Zum anderen bildet das System im Rahmen des Trainings Korrelationen zwischen den Trainingsdaten heraus, die sich anschließend nicht mehr entfernen lassen. In der Folge können Dritte bei der Nutzung des Systems die gespeicherten Korrelationen ausnutzen, um die Trainingsdaten zumindest

partiell zu rekonstruieren. Im Zusammenwirken mit den weitreichenden Möglichkeiten einer Reidentifikation betroffener Personen können so höchst sensible Rückschlüsse auf Einzelne gezogen werden.

Gleichwohl sieht § 303e Abs. 4 Satz 1 SGB V i.V.m. § 18 Abs. 1 Nr. 5 FDZ-GesV selbst für die besonders sensible Bereitstellung pseudonymisierter Einzeldatensätze nach wie vor nur eine Plausibilitätsprüfung des Zugangsantrags durch das Forschungsdatenzentrum vor. Diese Einschränkung des behördlichen Prüfungsrahmens ist beim heutigen Rechtsstand noch weniger akzeptabel als bereits zuvor. Sie trägt den hohen Risiken der neuen Nutzungszwecke nach § 303e Abs. 2 Nr. 9 und 10 SGB V nicht ansatzweise Rechnung. Angesichts der vorwiegend kommerziellen und anwendungsbezogenen Ausrichtung dieser Nutzungszwecke ist zudem die Wissenschaftsfreiheit nicht berührt, die früher – bereits damals nicht überzeugend – zur Rechtfertigung der bloßen Plausibilitätsprüfung herangezogen wurde.

Unzureichend ist als Schutzmechanismus die durch § 303e Abs. 3 Satz 3 SGB V eingeführte Möglichkeit für das Forschungsdatenzentrum, einen Antrag dem neu gebildeten Arbeitskreis zur Sekundärnutzung von Versorgungsdaten (§ 303d Abs. 2 SGB V) zur Stellungnahme zu der Plausibilität des Antrags vorzulegen. Denn zum einen steht die Vorlage im normativ nicht näher angeleiteten Ermessen des Forschungsdatenzentrums. Zum anderen ist die Stellungnahme des Arbeitskreises nicht verbindlich. Gerade für die potenziell besonders problematischen Nutzungszwecke nach § 303e Abs. 2 Nr. 9 und 10 SGB V ist ein Vetorecht eines unabhängigen, pluralistisch besetzten und fachkundigen Gremiums unabdingbar.

Schließlich regeln das SGB V und die FDZGesV nach wie vor nicht alle Fragen im Zusammenhang mit der Datenhaltung und Datennutzung, die angesichts der hohen Sensibilität der gespeicherten Daten einer abstrakt-generellen Festlegung durch verbindliches Außenrecht bedürfen. Insofern verweise ich auf die zusammenfassende Darstellung in meinem Schriftsatz vom 1. Februar 2023. Die jüngeren Rechtsänderungen haben den dort aufgeführten Defiziten nicht abgeholfen.

III. Widerspruchsrecht

In meinem Schriftsatz vom 1. Februar 2023 habe ich nochmals ausführlich begründet, dass den betroffenen Personen ein voraussetzungsloses Widerspruchsrecht gegen die Sekundärnutzung der auf sie bezogenen Daten im Datentransparenzverfahren zustehen muss.

Hieran ist auch in Anbetracht der Stellungnahme festzuhalten, die sich gegen ein solches Widerspruchsrecht wendet. Es mag zutreffen, dass nicht-zufällige Verteilungen von Widersprüchen die Aussagekraft der gespeicherten Daten mit Blick auf manche Auswertungsprojekte vermindern können. Das Anliegen einer möglichst validen Datenbasis für Forschungsprojekte geht jedoch dem gegenläufigen Interesse der betroffenen Personen an einem wirksamen Schutz ihrer Grundrechte nicht automatisch und generell vor. Deutlich wird dies etwa in der von der Stellungnahme hervorgehobenen Fallkonstellation einer seltenen Erkrankung, bei der schon einzelne Widersprüche die Validität des Datenbestands vermindern könnten. Gerade in dieser Fallkonstellation dürfte regelmäßig eine besondere Situation vorliegen, in der sich ein Widerspruchsrecht bereits aus Art. 21 Abs. 1 und Abs. 6 DSGVO ergibt. Die Beigeladene zu 4 hat im vorliegenden Verfahren selbst stets vorgebracht, dass dieses Widerspruchsrecht auch im Rahmen des Datentransparenzverfahrens zu beachten ist.

Im Übrigen lässt sich ein angemessener Ausgleich zwischen den betroffenen Interessen durch eine differenzierte Regulierung des Widerspruchsrechts herstellen, wie ich bereits in meinem Schriftsatz vom 1. Februar 2023 ausgeführt habe. Beispielsweise könnte das Widerspruchsrecht auf sensible Datenverarbeitungsformen wie die Bereitstellung pseudonymisierter Datensätze beschränkt und/oder für die unterschiedlichen Nutzungszwecke unterschiedlich weitreichend geregelt werden, etwa indem den betroffenen Personen bei einer Datennutzung zur Entwicklung von Arzneimitteln oder Systemen der Künstlichen Intelligenz ein weitergehendes Widerspruchsrecht eingeräumt wird als bei der Grundlagen- oder Versorgungsforschung. Insoweit besteht nach Auffassung der Klägerin ein Gestaltungsspielraum des Gesetzgebers. Die gegenwärtige Ausgestaltung des Datentransparenzverfahrens macht eine solche differenzierte Regulierung allerdings unmöglich, da die Klägerin wegen der Zentralisierung der Datenhaltung und des Fehlens eines Kommunikationskanals zwischen dem Forschungsdatenzentrum und den betroffenen Personen faktisch nur entweder der Übermittlung der auf sie bezogenen Daten an die Datensammelstelle insgesamt widersprechen kann oder jegliche Datenverarbeitung im Datentransparenzverfahren hinnehmen muss.

Dass die Forderung der Klägerin nach einem allgemeinen, also nicht auf besondere persönliche Situationen beschränkten Widerspruchsrecht nicht überzogen ist, zeigt auch der internationale Vergleich. Bereits in meinem Schriftsatz vom 1. Februar 2023 habe ich auf die *Opt-Out*-Modelle im Vereinigten Königreich hingewiesen, das als einer der führenden Standorte für die For-

schung mit Gesundheitsdaten weltweit gilt. Auch etwa das gleichfalls als vorbildlich geltende finnische Findata-System sieht ein *Opt Out* der betroffenen Personen vor,

> vgl. https://findata.fi/en/faq/how-can-i-prohibit-the-secondary-use-of-my-data.

Das taiwanische Verfassungsgericht hat in einer viel beachteten Grundsatzentscheidung die dortigen Regelungen zur Sekundärnutzung der Datenbestände der gesetzlichen Krankenversicherung insoweit beanstandet, als den betroffenen Personen kein Widerspruchsrecht eingeräumt wurde,

> Verfassungsgericht der Republik China, Urteil 111-Hsien-Pan-13 vom 12. August 2022; eine englischsprachige Zusammenfassung ist abrufbar unter https://cons.judicial.gov.tw/en/docdata.aspx?fid=5535&id=347736.

Im Übrigen sehen auch die ab 2029 geltenden Regelungen über die sekundäre Datennutzung im Rahmen des europäischen Gesundheitsdatenraums ein voraussetzungsloses und grundsätzlich umfassendes Widerspruchsrecht der betroffenen Personen vor,

> vgl. Art. 71 der Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847.

Prof. Dr. Matthias Bäcker, LL.M.