grundsätzlich auf die mündliche Verhandlung des Gerichts beschränkt und erfasst beispielsweise nicht die vom Gericht angeordnete Untersuchung durch einen Sachverständigen außerhalb der mündlichen Verhandlung[52].

VII. Zusammenfassendes Ergebnis

Die Hausarztzentrierte Versorgung erhält zwar eine immer größere Bedeutung. Sie ist dem Grunde nach auch erwünscht; die inhaltliche Ausgestaltung ist jedoch zum Teil rechtswidrig. Insbesondere sind die HZV-Verträge rechtswidrig, soweit sie den HZV-Verbänden im weiteren Sinne zugeordnet sind. Sie verstoßen zum einen in dem Vertragswortlaut in § 73b SGB V gegen die Satzungen der Hausarztverbände und der Krankenkassen, sie verstoßen aber auch gegen den Grundsatz des Vorbehalts des Gesetzes, mithin gegen staatsorganisatorische Grundsätze.

Mangels Vorhandenseins einer Ermächtigungsgrundlage ist es unzulässig, wenn außergerichtliche Kündigungen durch die regionalen Hausarztverbände oder den Deutsche Hausarztverband e. V. oder die Hausärztliche Vertragsgemeinschaft AG oder die HÄVG Rechenzentrum GmbH und eben nicht durch die Krankenkassen selber ausgesprochen werden. Auch bei gerichtlichen Überprüfungen von Kündigungen sind nur die Krankenkassen passivlegitimiert, nicht jedoch die vorbenannten Hausarztverbände.

52) Vgl. *Pitz* in: *Schlegel/Voelzke*, jurisPK-SGG, 2. Aufl., § 73 SGG, Rdnr. 44 (Stand: 15. 6. 2022).

https://doi.org/10.1007/s00350-023-6458-0

Anonymisierung von Patientendaten durch Fremdlabore für Dritte

Zur anonymisierenden Wirkung der Pseudonymisierung; datenschutzrechtliche Darstellung anhand eines Fallbeispiels

Paul C. Johannes und Christian L. Geminn*

Medizinische Diagnostik findet oft in einem Netzwerk statt. Proben oder Gesundheits(roh)daten werden von Ärztinnen und Ärzten erhoben und von diesen an Fremdlabore zur Diagnostik weitergeleitet. Diese Labore bedienen sich dann oft weiterer Dienste, um Verfahren zu beschleunigen oder Ergebnisse zu verbessern (Dritte). Der Beitrag betrachtet die datenschutzrechtlichen Implikationen dieses Vorgehens aus der Perspektive eines Fallbeispiels aus der Blutbildanalyse (I.) und eines entsprechenden Systemsaufbaus zur Datenübermittlung (II.). Die rechtliche Bewertung (III.) fokussiert sowohl darauf, ob eine Anonymisierung als Verarbeitungsvorgang erlaubnispflichtig ist (1.) als auch darauf, ob eine Pseudonymisierung gegenüber Dritten eine anonymisierende Wirkung haben kann (2.). Im Anschluss wird knapp auf weitere datenschutzrechtliche Pflichten eingegangen (IV.).

I. Zum Einsatz von Fremdlaboren zur Entscheidungsunterstützung

Arztpraxen werden häufig in der Diagnose durch Fremdlabore unterstützt. Auch diese Labore bedienen sich Dritter. Zur Übermittlung kommen dabei Webanwendungen zum Einsatz. Diagnostiker können diese Anwendungen als Entscheidungsunterstützungssysteme bei der Erstellung quantifizierter Differenzialdiagnosen und der damit verbundenen Beurteilung der klinischen Ergebnisse nutzen. Die Anbieter dieser Anwendungen setzen statistische und maschinelle Lernverfahren ein, um klinische, molekulare und medizinische Bild- oder Befunddaten zu integrieren und zu analysieren. Die entwickelten Modelle dienen der Erkennung von Krankheiten sowie der Identifizierung potenzieller Marker. Zum Beispiel werden Diagnostiker bei der Erkennung hämatologischer Neoplasien anhand der Analyse von Immunphänotypisierungsdaten aus durchflusszytometrischen Messungen (sog. FCS- oder LMD-Dateien; sog. Rohdaten) aus Zellsuspensionen durch eine automatisierte Diagnoseempfehlung unterstützt[1].

Hierzu werden die durchflusszytometrischen Rohdaten mit Standardverfahren ohne Beteiligung der Dritten erhoben. Diese Dateien werden anschließend vom medizinischen Labor in eine Webschnittstelle hochgeladen. Der Anbieter der Anwendung (Dritter) analysiert Daten und stellt die Ergebnisse den nutzenden medizinischen Laboren als Hilfestellung bei der Erstellung einer quantifizierten Differenzialdiagnose zur Verfügung. Diese können nach Einsicht in die Ergebnisdaten die vom Dritten berechneten klinischen Indikationen verwenden, um einen Diagnosebericht zu erstellen.

Die Anwendung zeigt nach der Analyse Wahrscheinlichkeiten für das Vorliegen oder Nichtvorliegen verschiedener hämatologischer Neoplasien an. Außerdem werden sogenannte Zytogramme nach Industriestandard, die der Nutzer für konventionelle Diagnosen verwendet, und zusätzliche von dem Dritten berechnete Indikationen wie Biomarker und Vergleichsdaten zu anderen Patientengruppen angezeigt. Eine endgültige Schlussfolgerung durch den Diagnostiker erfolgt in der Regel in einem Diagnosebericht.

Rechtsanwalt Paul C. Johannes, LL.M., Wiss. Mitarbeiter und Priv.-Doz. Dr. iur. Christian L. Geminn, Wiss. Mitarbeiter, Universität Kassel,
Pfannkuchstr. 1, 34109 Kassel, Deutschland

*) Die Autoren sind Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. Der Beitrag entstand auf Basis von Arbeiten zu einem Privatgutachten der Datenrecht Beratungsgesellschaft.

1) Ein anderes Beispiel für die Einbindung von Dritten ist z. B. die Unterbeauftragung von Speziallaboren durch ein Labor; andere Anwendungsbeispiele für Entscheidungsunterstützung sind z. B. die Vorhersage der Resistenz gegen Antibiotika aus massenspektrometrischen Datensätzen; s. mit weiteren Beispielen zum Einsatz von KI-Verfahren *Stumpe/Kirchhoff*, Diagnoseunterstützung durch künstliche Intelligenz für Labordaten, in: *Pfannstiel* (Hrsg.), Künstliche Intelligenz im Gesundheitswesen, 2022, S. 505 ff.

II. Fallbeispiel: Systemaufbau

Zur Darstellung der datenschutzrechtlichen Fragen dient der im Folgenden vorgestellte, beispielhafte Systemaufbau: Die in hämatologischen Speziallaboren oder Arztpraxen mit Laboren durch durchflusszytometrische Prozesse gewonnenen Rohdaten werden in standardisiertem Dateiformat durch die Labormitarbeiter hochgeladen. Hierfür nutzen sie die durch den Anbieter des Systems zur Entscheidungsunterstützung angebotene Anonymisierungsfunktion.

Die Anonymisierung der Dateien (sog. FCS- oder LMD-Dateien) wird clientseitig im Browser des Kunden (medizinische Labore) durchgeführt. Die zu anonymisierenden Daten verlassen dabei vor der Anonymisierung nicht das Endgerät des Kunden und werden nicht an Server des Anbieters übermittelt.

Den zur Übermittlung vorgesehenen FCS- und LMD-Dateien werden durch diese Anonymisierungsfunktion identifizierende Merkmale entfernt, wie zum Beispiel Name, Vorname, Alter, Geschlecht, Anschrift, Kontaktdaten, Versichertennummer und sonstige Identifier. Welche Identifier verwendet und gelöscht werden, kann sich von Labor zu Labor oder Arztpraxis zu Arztpraxis unterscheiden. Den Dateien wird dann anwendungsseitig eine randomisierte ID zugeordnet, sodass es dem Kunden möglich ist, die Analyseergebnisse später dem jeweiligen Patienten zuzuordnen. Diese wird anschließend verschlüsselt und dann erst an den Anbieter übertragen. Der Anbieter des Unterstützungssystems erhält diese Datei mit der verschlüsselten ID. Einzelne Patienten können dadurch weder vom Anbieter noch von einem sonstigen Dritten identifiziert werden. Nur noch der Kunde kann mit dem ihm vorliegenden Zuordnungsschlüssel einen Bezug zu einem Patienten herstellen, wenn der Anbieter die Daten zurücksendet. Dem Kunden, also dem Arzt oder dem Labor, ist es nicht gestattet, diese Zusatzinformationen herauszugeben[2].

Die Inhalte der an den Anbieter übermittelten hämatologischen Daten sind für sich gesehen keiner natürlichen Person eindeutig zuordenbar. Über sie lässt sich auch keine Person identifizieren. Die Inhalte variieren selbst bei einer einzelnen Person je nach Tagesform und Messungsinstrument und sehen nicht identisch aus. Sie sind anders als genetische Daten nicht eineindeutig einer Person zuzuordnen.

Der Anbieter hält die Daten auf seinen Servern (Cloud) vor, um sie den Kunden zur Auswertung zur Verfügung zu stellen und um das eigene Analysesystem zu trainieren. Es findet somit neben der eigentlichen Beauftragung auch eine eigennützige Verwendung der übermittelten Daten durch den Anbieter statt, was nicht durch ein Auftragsverarbeitungsverhältnis im Sinne von Art. 28 DSGVO legitimiert werden kann.

III. Rechtliche Bewertung

1. Ist die Anonymisierung selbst erlaubnispflichtig?

a) Was ist unter Anonymisierung zu verstehen?

Die Datenschutz-Grundverordnung definiert zwar die Pseudonymisierung (Art. 4 Nr. 5 DSGVO), nicht aber die Anonymisierung[3]. Trotzdem besteht weitgehend Einigkeit darüber[4], das anonymisieren bedeutet, personenbezogene Daten so zu verändern, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können[5]. Anonyme Daten sind das genaue Gegenteil von personenbezogenen Daten[6]. Sie grenzen sich definitorisch von diesen dadurch ab, dass sie gerade keine personenbezogenen Daten sind[7]. Anonymisierung und Personenbezug korrelieren insofern negativ[8]. Entscheidend ist, dass die Daten zwar Angaben zu einer bestimmten Person enthalten können, dass mit ihnen aber kein Bezug zu einer identifizierten oder identifizierbaren natürlichen Person hergestellt werden kann.

b) Anonymisierung als Verarbeitungsvorgang

Die Anonymisierung von personenbezogenen Daten ist nach herrschender Meinung eine Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO[9]. Diesen Standpunkt vertreten auch Aufsichtsbehörden[10]. Als Verarbeitung bedarf die Anonymisierung wegen des Grundsatzes des Vorbehalts des Gesetzes[11] einer rechtlichen Grundlage (Erlaubnis), die sich im Wesentlichen aus Art. 6 DSGVO ergeben muss[12]. Die Anonymisierung personenbezogener Daten dürfte überwiegend nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zulässig sein, weil durch die Anonymisierung schutzwürdige Rechte der betroffenen Person selten oder in geringem Maß berührt sein dürften[13]. Sie kann ganz im Gegenteil gerade dem Schutz dieser Interessen dienen und im Falle medizinischer Diagnostik eine Verarbeitung, die in besonderem Maße im Interesse der betroffenen Peron liegt, zusätzlich absichern. Es ist aber auch denkbar, dass durch die Anonymisierung insbesondere im Vergleich zur Löschung zusätzliche Risiken für die betroffene Person entstehen.

c) Implikationen für Laboruntersuchungen

Bei Daten besonderer Kategorien im Sinne von Art. 9 Abs. 1 DSGVO muss die Verarbeitung zusätzlich nach Art. Art. 9 Abs. 2 DSGVO erlaubt sein. Die von den Laboren im Fallbeispiel verarbeiteten hämatologischen Daten sind Gesundheitsdaten. Die Verarbeitung von Gesundheitsdaten ist nach Art. 9 Abs. 2 lit. h und Abs. 3 DSGVO in Verbindung mit § 22 Abs. 1 Nr. 1 lit. b BDSG erlaubt, wenn dies zu Zwecken der medizinischen Diagnostik oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist. Bedingung ist, dass diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung

2) § 203 StGB; s. hierzu und insbesondere zum Verhältnis zum Datenschutzrecht *Geminn*, RDV 2019, 116.
3) Sie unterstellt diese aber z. B. in Art. 5 Abs. 1 lit. c und 89 Abs. 1 S. 4 DS-GVO und erwähnt sie in Erwägungsgrund 26 S. 5 und 6 DSGVO.
4) Vgl. z. B. *Roßnagel*, ZD 2021, 188 (189); *Gierschmann*, ZD 2021, 482 f.; *Gola*, in: *Gola/Heckmann* (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, Art. 4, Rdnr. 51.
5) Ebenso z. B. die Definitionen in § 3 BbgDSG, § 2 Abs. 4 BremDSG, § 11 Abs. 2 HmbDSG, § 2 Abs. 4 HDSIG, § 4 DSG NRW; § 24 Nr. 18 NDSG, § 3 Abs. 2 Satz 2 Nr. 4 Sächs. DSG, § 2 Abs. 7 DSG LSA; § 13 Abs. 2 DSG SH, § 28 Abs. 3 ThürDSG.
6) S. z. B. *Klar/Kühling*, in: *Kühling/Buchner* (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 4, Rdnr. 32.
7) S. *Hofmann/Johannes*, ZD 2017, 223.
8) *Roßnagel/Scholz*, MMR 2000, 721, 723.
9) S. *Roßnagel*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, 2019, Art. 4 Nr. 2, Rdnrn. 12, 14, 32; *Hornung/Wagner*, ZD 2020, 223; *Roßnagel*, ZD 2021, 188, 189; a. A. *Thüsing/Rombey*, ZD 2021, 548; zum Meinungsstand *Gierschmann*, ZD 2021, 482, 484.
10) Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 2020; zustimmend Stellungnahmen LfDI BW, LfDI NRW; anders LfD SA; s. https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/Positionspapier-Anonymisierung-DSGVO-TKG.html.
11) S. hierzu *Roßnagel*, NJW 2019, 1.
12) S. *Ziebarth*, in: *Sydow/Marsch* (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, Art. 4, Rdnrn. 97 f.; *Husemann*, in: *Roßnagel* (Hrsg.), Das neue Datenschutzrecht, 2018, § 3, Rdnr. 7; *Roßnagel*, in: *Roßnagel* (Hrsg.), HDSIG, 2021, § 2, Rdnrn. 40 ff.
13) S. z. B. *Hornung/Wagner*, ZD 2020, 223; *Roßnagel*, ZD 2021, 188, 189.

verarbeitet werden. Im Rahmen der ärztlichen Behandlung und der medizinischen Diagnostik in einem Labor unter laborärztlicher Aufsicht bedarf es in der Regel keiner zusätzlichen Einholung einer datenschutzrechtlichen Einwilligung beim Patienten hinsichtlich der Laboruntersuchung und der entsprechenden Datenübermittlung vom Arzt an das Labor.

Ob die Anonymisierung von Labordaten zur weiteren Übermittlung an Dritte von dieser Erlaubnis oder dem Vertragszweck getragen werden kann, ist fraglich. Gerade in der Weitergabe der Daten verstärkt sich das Risiko einer Re-Identifizierung; sie negiert damit möglicherweise sogar den Vorteil, den die betroffene Person durch eine Anonymisierung ihrer Daten als technische Sicherungsmaßnahme hätte. Deswegen wird angenommen, dass besondere Kategorien personenbezogener Daten in der Regel[14] nur mit Einwilligung gem. Art. 9 Abs. 1 lit. a DSGVO anonymisiert werden können, was wertungswidersprüchlich ist[15]. Ein Teil der Literatur will dieses Problem über eine teleologische Reduktion von Art. 9 DSGVO lösen[16]. Der unionale Gesetzgeber habe das Problem der fehlenden Rechtsgrundlage für das Löschen und Vernichten (und damit das Anonymisieren) sensibler Daten schlicht übersehen. Deshalb sei Art. 9 DSGVO für Löschung, Vernichtung und Anonymisierung teleologisch zu reduzieren, sodass sich die Erlaubnis generell nach Art. 6 Abs. 1 DSGVO richte. Die rechtswissenschaftliche Diskussion hierzu ist aber nicht abgeschlossen.

Aus Gründen der Rechtssicherheit ist deswegen ratsam, entweder (1) den Patienten in die Anonymisierung von Gesundheitsdaten zur Weitergabe durch ein Fremdlabor ausdrücklich einwilligen zu lassen oder (2) eine Anonymisierung und Weitergabe der anonymisierten Daten durch das Fremdlabor an Dritte ausdrücklich zum Gegenstand des Behandlungs- oder des Diagnostikvertrags zu machen (zum Beispiel in der Leistungsbeschreibung). Letzteres wäre vorteilhaft, insoweit ein separates Einwilligungsmanagement beim Diagnostiklabor entfiele.

So oder so hat der Verantwortliche, hier also zum Beispiel ein Diagnostiklabor, außerdem vor einer Anonymisierung die betroffene Person über die Zwecke, für die die personenbezogenen Daten anonymisiert werden sollen, zu informieren sowie ihr die Rechtsgrundlage für die Anonymisierung mitzuteilen.

2. Sind die an Fremdlabore oder Dritte übermittelten Daten nach geltendem Recht anonymisiert?

a) Pseudonymisierung durch die Labore

Pseudonymisieren ist nach Art. 4 Nr. 5 DSGVO die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Durch die Entfernung identifizierender Merkmale unter Hinzufügung einer randomisierten ID können Labore den zur Übermittlung an den Anbieter eines Unterstützungssystems bestimmten Datensatz pseudonymisieren. Über die ID können die Labore den Personenbezug stets wiederherstellen.

b) Anonymisierende Wirkung der Pseudonymisierung

Fraglich ist, ob diese Pseudonymisierung bei den Laboren in Bezug auf den Anbieter eines Systems zur diagnostischen Entscheidungsunterstützung eine anonymisierende Wirkung hat. Anonyme oder anonymisierte Daten unterliegen nicht (mehr) der Datenschutz-Grundverordnung oder den Datenschutzgesetzen des Bundes und der Länder.

Nach der von einem Teil der Literatur vertretenen Meinung soll Pseudonymisierung keinen Einfluss auf die Personenbeziehbarkeit eines Datums haben[17]. Sie sei bestenfalls eine technisch-organisatorische Maßnahme zum Schutz der weiterhin personenbezogenen Daten[18].

Nach zutreffender und wohl herrschender Meinung kann einer Pseudonymisierung eine anonymisierende Wirkung gegenüber demjenigen zukommen, der die Zuordnungsregel zwischen Pseudonym und den von ihm ersetzten identifizierenden Merkmalen nicht kennt[19]. Die Bewertung der Anonymität bestimmter Daten ist also vom konkreten Verarbeitungskontext abhängig. Diese Bewertung kommt auch schon in der EuGH-Rechtsprechung zum Tragen[20]. Der EuGH hatte zu entscheiden, ob IP-Adressen personenbezogene Daten sind. Dabei hat das Gericht allgemein festgestellt, dass das Wissen anderer Personen oder Stellen für den Verantwortlichen ein Mittel darstellt, das dieser „vernünftigerweise" zur Bestimmung der betreffenden Person einsetzen kann, wenn er über rechtliche Möglichkeiten verfügt, um an das identifizierende Zusatzwissen zu gelangen. Ein Mittel kann dagegen nicht „vernünftigerweise" zur Bestimmung einer natürlichen Person eingesetzt werden, wenn die Identifizierung der Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, sodass das Risiko einer Identifizierung de facto vernachlässigbar erschiene[21]. Auch wenn sich das Urteil noch auf die Datenschutz-Richtlinie (RL 1995/46/EG – DS-RL) bezog, haben die dort getroffenen Erwägungen Gewicht, insbesondere weil die Definition in Art. 2 lit. a DS-RL sowie Erwägungsgrund 26 fast wortgleich in die DSGVO übernommen worden sind[22].

Anonymisieren bedeutet das Verändern personenbezogener Daten dergestalt, dass die Einzelangaben über per-

14) Anonymisierung zu Übermittlung kann auch nach bereichspezifischen Normen erlaubt sein, zum Beispiel für die Verarbeitung zu wissenschaftlichen Zwecken nach § 27 Abs. 1 BDSG in Verbindung mit Art. 9 Abs. 2 lit. j DSGVO und Art. 89 Abs. 1 DSGVO, wenn die Anonymisierung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Anonymisierung und Übermittlung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.

15) *Gierschmann*, ZD 2021, 482, 485.

16) *Hornung/Wagner*, ZD 2020, 223.

17) *Eckhardt/Kramer*, DuD 2013, 287, 288 f.; *Karg*, DuD 2015, 520, 521 f.; PDK Hessen § 2, Rdnr. 17; *Schild*, in: BeckOK DatenschutzR, 42. Ed. 1.11.2022, DSGVO, Art. 4, Rdnr. 77; *Ernst*, in: *Paal/Pauly*, DS-GVO/BDSG, 3. Aufl 2021, Art. 4, Rdnr. 40; *Piltz*, K&R 2016, 557, 562; *Klar/Kühling*, in: *Kühling/Buchner*, DS-GVO/BDSG, 3. Aufl. 2020, Art. 4, Rdnrn. 26 ff., 31.; nach *Weichert*, in: *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 4, Rdnr. 80, soll die Datenverarbeitung weiterhin der DSGVO unterliegen, wenn die Re-Identifizierung nicht absolut ausgeschlossen ist.

18) *Karg*, DuD 2015, 520, 521 f.; *Albrecht/Jotzo*, DatenschutzR, 2017, Teil 3, Rdnr. 4, Teil 5, Rdnr. 8.

19) Mit weiteren Nennungen, insb. zum BDSG a. F., *Ziebarth*, in: *Sydow/Marsch* (Hrsg.), DS-GVO/BDSG, 2022, Art. 4, Rdnrn. 97 f.; s. a. *Bischoff*, PharmR 2020, 309, 314; *Roßnagel*, ZD 2018, 243, 245 f.; *Eßer*, in: *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, 7. Aufl. 2020, Art. 4, Rdnr. 71; *Gierschmann*, ZD 2021, 482, 483; *Hofmann/Johannes*, ZD 2017, 221, 224; *Johannes*, in: *Roßnagel* (Hrsg.), Das neue Datenschutzrecht, 2018, § 7, Rdnr. 249; *Pötters*, in: *Gola/Heckmann* (Hrsg.), DS–GVO/BDSG, 3. Aufl. 2022, Art. 89, Rdnr. 13.

20) EuGH, ZD 2017, 24 m. Anm. *Kühling/Klar – Breyer* = ECLI:EU:C:2016:779.

21) EuGH, ZD 2017, 24, Rdnrn. 46 ff.

22) Vgl. Erwägungsgrund 26 S. 4 DSGVO.

sönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Für die Feststellung einer Identifizierbarkeit der betroffenen Person ist Art. 4 Nr. 1 DSGVO zufolge maßgeblich, ob die vorhandene Information als solche bereits für eine Identifizierung ausreicht oder ob die Heranziehung oder Verknüpfung weiterer Informationen zur Bestimmung erforderlich ist. Hierbei sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die betroffene Person zu identifizieren. Entscheidend ist daher, ob der Verantwortliche mittels der ihm zur Verfügung stehenden Mittel, Kenntnisse und Möglichkeiten im Rahmen einer Ermessensentscheidung und Verhältnismäßigkeitsabwägung die Identifikation vornehmen kann.

c) Risikoprognose zur Re-Identifizierung

Nach dem relativen Konzept des Personenbezugs[23] ist in einer Risikoprognose zu bestimmen, die sowohl das Interesse möglicher Datenverarbeiter als auch die von ihnen mobilisierbaren Mittel der Zuordnung berücksichtigt, ob die nach der Anonymisierung verbleibenden Daten personenbeziehbar sind.[24] Ihre Zuordnung zu einer identifizierbaren Person muss im Verhältnis zu dem dazu notwendigen Aufwand so unverhältnismäßig sein, dass eine Identifizierung nach allgemeiner Lebenserfahrung oder dem Stand der Wissenschaft und Technik nicht zu erwarten ist. Zu berücksichtigen sind dabei das vorhandene oder erwerbbare Zusatzwissen des Verantwortlichen, aktuelle und künftige technische Möglichkeiten der Verarbeitung sowie der mögliche Aufwand und die verfügbare Zeit. Ein absoluter Ausschluss der Zuordnung ist weder möglich noch erforderlich[25].

Bezogen auf die Diagnostiklabore sind die Daten somit pseudonym, bezogen auf den Anbieter des Unterstützungssystems und Dritte sind sie anonym. Unter den folgenden Voraussetzungen wären die durch die Labore pseudonymisierten Daten für den Anbieter anonymisiert:

- Der Anbieter verfügt über kein Zusatzwissen, die einzelnen Analysedatensätze einer bestimmten natürlichen Person zuzuordnen. Die randomisierte ID ermöglicht keinen Rückschluss auf eine natürliche Person, da sie nicht auf anderen personenbezogenen Daten der Patienten beruht. Nur dem einzelnen Labor ist eine Zuordnung möglich, da dieses die randomisierte ID mit den ihm vorliegenden Patientendaten verknüpfen kann. Außerdem kann die randomisierte ID vor Übermittlung an den Anbieter vom übermittelnden Labor verschlüsselt werden, so dass der Anbieter sogar nur die verschlüsselte ID kennen würde.
- Der Anbieter verfügt auch über keine rechtlichen Mittel an das Wissen zu den IDs bei den Laboren zu gelangen. Es dürften keine gesetzlichen oder vertraglichen Auskunftsrechte gegenüber den Laboren vorliegen.
- Die Informationen zur ID bei den Laboren sollten auch einer berufsrechtlichen Geheimhaltungspflicht unterliegen (ärztliche Schweigepflicht des Laborarztes).
- Der Anbieter darf auch in tatsächlicher Hinsicht nicht in der Lage sein, einzelne Personen anhand der übermittelten Daten zu re-identifizieren. Den übermittelten Analysedaten darf keine Information zur Identifizierung inhärent sein. Blutbilder von Patienten etwa sind Momentaufnahmen und (anders als zum Beispiel biometrische oder genetische Daten) nicht eindeutig und aussagekräftig genug, um eine Person individualisierbar zu machen.
- Der Anbieter hat auch keine tatsächliche Möglichkeit zur Einsichtnahme der Daten bei den Laboren, insbesondere nicht über die Anwendungskomponente. Die Anwendung erfolgt auf den Systemen der Labore.

Grundsätzliche wäre es zwar möglich, dass der Anbieter die Anwendungskomponenten, die er den Laboren zur Verfügung stellt, (heimlich) ändert und sich so zum Beispiel Zugriff zu den IDs verschafft. Damit würde der Anbieter aber gegen Vertragspflichten gegenüber den Laboren verstoßen. Zudem wären auch Straftatbestände erfüllt, weswegen das hiermit verbundene Risiko einer Re-Identifizierung vernachlässigbar ist. Der Einsatz rechtswidriger Mittel zur Re-Identifizierung ist nicht „nach allgemeinem Ermessen wahrscheinlich" im Sinne von Erwägungsgrund 26 DSGVO[26].

Das Risiko einer Re-Identifizierungen lässt sich jedoch nie vollständig ausschließen. Aufdeckungen des Personenbezugs lassen sich insbesondere dann nicht ausschließen, wenn die Daten vielen Verantwortlichen mit unterschiedlichem mobilisierbarem Zusatzwissen zur Verfügung stehen und langfristig aufbewahrt und damit dem künftigen technischen Fortschritt ausgesetzt sein werden. Wenn ausreichendes Vertrauen in die Anonymisierung und damit in die wesentliche Voraussetzung gerade auch für das Trainieren, Testen und Evaluieren von KI-Systemen erreicht werden soll, müssen ergänzende – insbesondere rechtliche – Maßnahmen in die Beständigkeit der Anonymität ergriffen werden[27]. Dies schließt angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person im Sinne von § 22 Abs. 2 BDSG ein, die dann auch darauf abzielen das Risiko einer Re-Identifizierung weiter zu verringern. Konkrete Beispiele für Maßnahmen, die ein entsprechender Anbieter treffen könnte sind:

- Verpflichtung von Mitarbeitern auf Wahrung von Geschäftsgeheimnissen und Datenschutz, die auch die Re-Identifizierung und ungenehmigte Weitergabe anonymisierter Daten umfassen;
- Prüfung der an den Anbieter übermittelten Daten durch den Anbieter bei Eingang darauf, dass identifizierende Merkmale durch das übermittelnde Labor entfernt wurden;
- Einschaltung eines Datentreuhänders oder Datenvermittlungsdienstes, der Zuordnungsschlüssel für Labore und Dritte verwaltet, die Qualität der Anonymisierung prüft und ggf. nicht benötigte identifizierende Merkmale entfernt;
- weitere Maßnahmen zur Anonymisierung der Datensätze, ggf. schrittweise oder nach bestimmten Fristablauf, zum Beispiel durch Löschung der ID zur Übernahme in KI-Trainingsdaten, Verschleierung oder Löschung von Metadaten zur Herkunft und Eingangszeitpunkt;
- Löschkonzept erstellen und einhalten.

23) S. ausführlich *Roßnagel/Geminn*, in: *Dierks/Roßnagel*, Sekundärnutzung von Sozial- und Gesundheitsdaten, 2019, S. 149 ff. m. w. N.

24) S. auch *Schwartmann/Jaspers/Lepperhof/Weiß/Meier*, Praxisleitfaden für die Anonymisierung personenbezogener Daten, 2022.

25) S. z. B. *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 v. 10. 4. 2014, WP 216, S. 10; *Gola*, in: *Gola/Heckmann*, DS-GVO/BDSG, 3. Aufl. 2022, Art. 4, Rdnr. 40; *Ziebarth*, in: *Sydow/Marsch* (Hrsg.), DS-GVO/BDSG, 2022, Art. 4, Rdnrn. 97 f.; *Husemann*, in: *Roßnagel* (Hrsg.), Das neue Datenschutzrecht, 2018, § 3, Rdnr. 7; *Roßnagel*, in: *Roßnagel* (Hrsg.), HDSIG, 2021, § 2, Rdnr. 40 ff.; *Roßnagel/Scholz*, MMR 2000, 721, 723 f.

26) *Pötters*, in: *Gola/Heckmann* (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, Art. 89, Rdnr. 12; *Karg*, in: *Simitis /Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, 2018, Art. 4 Nr. 1, Rdnr. 64; *Klar/Kühling*, in: *Kühling/Buchner* (Hrsg.), DSGVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 1, Rdnr. 29.

27) *Roßnagel/Geminn*, ZD 2019, 487, 488.

IV. Weitere Datenschutzrechtliche Pflichten für Fremdlabor und Dritte

Die Labore sind auch hinsichtlich des Anonymisierungsvorgangs mit datenschutzrechtlichen Verpflichtungen belegt – so hinsichtlich der den betroffenen Personen bereitzustellenden Informationen und bei konkreten Auskunftsbegehren von betroffenen Personen. Denn für die Labore haben die Daten noch Personenbezug, da sie über den Zuordnungsschlüssel oder Zusatzinformationen verfügen. Die Labore müssen also auch sicherstellen, dass die Anonymisierung und die Übermittlung der Daten durch Einwilligung der Patienten oder durch Vertrag im Verhältnis Arzt zu Labor legitimiert ist. Die die Daten weiterleitenden Labore sind in der Regel dazu verpflichtet eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, s. insbesondere Punkt 15 und 16 der Blacklist der Datenschutzaufsichtsbehörden[28]. Auch wenn man den Standpunkt vertritt, dass die Daten für den Drittanbieter anonym sind, so kann es für ihn dennoch sinnvoll sein bezogen auf die Verarbeitung dieser Daten eine DSFA durchzuführen. Nach Art. 35 Abs. 3 lit. b DSGVO wäre der Dritte bei „umfangreicher" Verarbeitung von Daten besonderer Kategorie dazu gezwungen. Eine DSFA könnten von dem Dritten auch werbewirksam genutzt werden. Die freiwillige Befolgung von datenschutzrechtlichen Pflichten wie etwa der Durchführung einer DSFA durch den Drittanbieter folgt der Überlegung, dass selbst bei anonymisierten Daten, bei denen anders als im hier dargestellten Fall keine Zuordnungsregel verbleibt, das Restrisiko einer De-Anonymisierung im Sinne einer Re-Identifizierung durch Unbefugte besteht. Hier ist insbesondere eine Nutzung der übermittelten anonymisierten Daten jenseits der konkreten Auswertung zu denken, etwa zur Verbesserung des Algorithmus. Um diesem Restrisiko zu begegnen, werden in der Literatur bereits seit längerer Zeit gesetzgeberische Maßnahmen gefordert – so etwa die Schaffung von klaren gesetzlichen Vorgaben für die Verwendung anonymisierter Daten wie beispielsweise einer Zweckbegrenzung[29]. Auch in Ermangelung solcher gesetzlicher Vorgaben bleibt aber eine freiwillige Befolgung ausgewählter datenschutzrechtlicher Verpflichtungen wie etwa der zur Durchführung einer DSFA zumindest empfehlenswert, um zusätzliches Vertrauen aufzubauen, denn die DSFA bedingt nicht nur eine kritische Bewertung der eigenen Prozesse, sondern auch die Zuordnung von konkreten Maßnahmen zu den erkannten Risiken.

V. Fazit

Das Konzept der anonymisierenden Wirkung der Pseudonymisierung verbreitet in der Praxis mitunter große Unsicherheit[30], die einerseits aus der Komplexität der Konstruktion, andererseits aus dem seit langem bestehenden Streit um das Konzept resultiert. Dabei darf nicht vergessen werden, dass es auch im Kontext der Anonymisierung nicht um eine Reduktion bestehender Risiken auf Null gehen kann. Ein Restrisiko der De-Anonymisierung besteht zumindest mit Blick auf möglicherweise in der Zukunft entstehende Auswertungsmethoden. Bezogen auf die anonymisierende Wirkung der Pseudonymisierung bestehen aber wirksame Instrumente in Form von technischen und organisatorischen Maßnahmen, um die verbleibenden Risiken zu adressieren. Um diese Maßnahmen zu identifizieren und bestmöglich zu interpretieren, bietet sich die DSFA als methodisch geleiteter Prozess an, der es erlaubt, die eigene Verarbeitungstätigkeit auf Herz und Nieren zu prüfen, Risiken zu erkennen und zu klassifizieren, und schließlich den Risiken je nach Schwere entsprechende technische und organisatorische Maßnahmen zuzuordnen. Empfohlen wird somit das Ergreifen von aus dem Datenschutzrecht bekannten Sicherungsmaßnahmen auch bei der Verarbeitung von Daten, die (bezogen auf den verarbeitenden Dritten) aus dem Geltungsbereich des Datenschutzrechts herausfallen. Hinzu sollten weitere, freiwillige Selbstverpflichtungen treten, insbesondere hinsichtlich einer Beschränkung der Verarbeitung der anonymisierten Daten auf festgelegte und eng definierte Zwecke. So kann schließlich das gerade bei Gesundheitsdaten notwendige Vertrauen in die sichere Handhabung der Daten geschaffen werden. Noch besser wäre es, wenn der Gesetzgeber entsprechende Vorgaben zum Umgang mit anonymisierten Daten schaffen würde.

Open Access funding enabled and organized by Projekt DEAL.

28) Abrufbar unter: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf.
29) S. z. B. *Roßnagel/Geminn*, ZD 2019, 487, 489 f.
30) Exemplarisch zur Tatsachenfrage der Möglichkeit der Re-Identifizierung beim Hamburger Krebsregister die ausführliche Darstellung und Bewertung in VG Hamburg, Urt. v. 28. 7. 2022 – 21 K 1802/21 = BeckRS 2022, 35319.