Personenbezogene Daten im Kontext biomedizinischer Sekundärforschungsnutzung

Markus Spitz und Kai Cornelius

1 Praktische und rechtliche Ausgangslage

Die aus dem Arzt-Patienten-Kontext stammenden klinischen Daten sind für die biomedizinische Forschung von entscheidender Bedeutung.¹ Wegen des sensiblen Kontextes birgt die sekundäre Nutzung dieser Daten indes informationelle Risiken für den Betroffenen. Die Verarbeitung klinischer Daten zu Forschungszwecken unterliegt daher einem umfangreichen rechtlichen Schutzregime. Die Grundlagen dieses Schutzes ergeben sich primär aus dem allgemeinen und bereichsspezifischen Datenschutzrecht.² Das allgemeine Datenschutzrecht stellt die klinischen Daten (als Teil von Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO³ sowie genetischen Daten nach Art. 4 Nr. 13 DSGVO) unter den besonderen Schutz des Art. 9 Abs. 1 DSGVO.

¹ Zur Definition klinischer Daten, die für Forschungs- und Lernaktivitäten sekundär genutzt werden, vgl. in diesem Band *Jungkunz et al.*

² *Weichert*, ABIDA Gutachten Big Data im Gesundheitsbereich, 2018, S. 109 f.

³ 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), ABl. L 119 S. 1.

M. Spitz (✉)

Juristische Fakultät, Universität Heidelberg, Heidelberg, Deutschland

E-Mail: markus.spitz@jurs.uni-heidelberg.de

K. Cornelius

Heidelberg, Deutschland

E-Mail: kai.cornelius@jurs.uni-heidelberg.de

Voraussetzung für diesen Schutz ist stets, dass *personenbezogene Daten* gem. Art. 2 Abs. 1 DSGVO verarbeitet werden. Handelt es sich bei den verarbeiteten Daten dagegen nicht um personenbezogene oder anonyme Daten, entfällt der datenschutzrechtliche Schutz.⁴ Das personenbezogene Datum hat folglich Scharnierfunktion. Es wird als der wichtigste Begriff des Datenschutzrechts bezeichnet, da es darüber entscheidet, ob das Datenschutzrecht in seiner Gesamtheit anwendbar ist oder nicht.⁵

Vergleichbares gilt für die zahlreichen bereichsspezifischen Vorschriften. Auch hier ist das personenbezogene Datum maßgeblicher Anknüpfungspunkt, etwa im Bereich der landesrechtlichen Krankenhausgesetze (beispielsweise nach § 43 Abs. 4 LKHG BW⁶) oder im Sozialdatenschutz nach § 67 Abs. 2 S. 1 SGB X⁷. Für den Verantwortlichen, der klinische Daten sekundär zu Forschungszwecken verarbeitet, ist die Frage des Personenbezugs somit entscheidend. Sind die von ihm verarbeiteten Daten nicht personenbezogen, unterfällt er nicht den rechtlichen Pflichten des Datenschutzrechts. Er muss in diesem Fall keine Einwilligung für die Verarbeitung der nicht personenbezogenen Daten einholen oder sonstige datenschutzrechtliche Pflichten (etwa Informationspflichten oder Pflichten zur Datenschutzfolgenabschätzung) erfüllen. Bevor eine Untersuchung von datenschutzrechtlichen Pflichten erfolgt ist daher zu klären, was überhaupt als personenbezogenes Datum einzuordnen ist.⁸

2 Die Reichweite des Personenbezugs bei Daten

Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.⁹ Das ist bei Informationen der Fall, durch die natürliche Personen direkt oder indirekt, insbesondere mittels Zuordnung zu weiteren Identifikationsmerkmalen (Kennnummern, Standortdaten etc.) identifiziert werden können. Diese grundlegende Anforderung gilt auch im Fall der Verarbeitung von Gesundheitsdaten gem. Art. 4 Nr. 15 DSGVO oder genetischen Daten gem. Art. 4 Nr. 13 DSGVO. Direkt oder indirekt, insbesondere mittels Zuordnung bedeutet, dass eine für sich genommen nicht identifizierende Information durch die Verknüpfung

⁴ Weichert, ABIDA Gutachten Big Data im Gesundheitsbereich, 2018, S. 140

⁵ Dammann, in: Simitis (Hrsg.), BDSG a.F., 8. Aufl. 2014, § 3 Rn. 3.

⁶ Landeskrankenhausgesetz Baden-Württemberg (LKHG BW) vom 15. Dezember 1986 in der Fassung vom 29. November 2007, GBl. 2008 S. 13.

⁷ Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) in der Fassung vom 18. Januar 2001, BGBl. I S. 130.

⁸ Schneider, Sekundärnutzung klinischer Daten, 2015, S. 11.

⁹ Zur Auslegung der einzelnen Merkmale unter der Datenschutzrichtlinie Art.-29-Datenschutzgruppe, WP 136, 4/2007, S. 6 ff.

mit zusätzlichem Wissen zu einem personenbezogenen Datum werden kann (Identifizierbarkeit). Umstritten ist dabei, ob diese Verknüpfungsmöglichkeit mit Zusatzwissen nur dann beachtlich ist, wenn solches Zusatzwissen beim Verantwortlichen (Forscher) selbst vorliegt oder auch, wenn dieses Wissen ausschließlich bei Dritten, etwa der behandelnden Stelle oder einer Datentreuhandstelle, verfügbar ist. Die Frage der Zurechnung von solchem Drittwissen stellt sich gerade in der biomedizinischen Forschung aufgrund der häufigen Nutzung von Pseudonymisierungsmethoden, bei denen Zusatzwissen (wie der Pseudonymisierungsschlüssel) von den zu beforschenden Daten getrennt und bei unterschiedlichen Stellen aufbewahrt werden.¹⁰ Der Streit um die Zurechenbarkeit von Zusatzwissen soll im Folgenden vor dem Hintergrund des datenschutzrechtlichen Vorfeldschutzes näher untersucht werden.

2.1 Das Merkmal der Identifizierbarkeit

Einer tatsächlichen Identifikation oder auch nur einer Identifikationsabsicht bedarf es für die Identifizierbarkeit nicht.¹¹ Das Tatbestandsmerkmal der Identifizierbarkeit stellt eine Vorverlagerung des datenschutzrechtlichen Schutzes für eine Situation dar, in der die natürliche Person noch nicht identifiziert ist (datenschutzrechtlicher Vorfeldschutz).¹² Zweck des Datenschutzrechts ist der Schutz des Einzelnen vor den Gefahren, die aus dem Wissen Dritter über seine Person folgen.¹³ Gerade Gesundheitsdaten, insbesondere auch in Form genetischer Daten, können in den falschen Händen Gefahren für Betroffene materieller und immaterieller Art begründen.¹⁴ Dabei kennt der Betroffene oft gar nicht im Detail das Wissen Dritter über seine Person. Bei der Verarbeitung von Gesundheitsdaten und speziell genetischer Daten ist das Wissen Dritter das Resultat von für den Betroffenen häufig im Verborgenen ablaufenden Interpretations- und Bewertungsprozessen.¹⁵ Aufgrund der damit einhergehenden Gefahren schützt das Datenschutzrecht die betroffene Person schon vor dem Moment der eigentlichen Identifikation vor einer möglichen Persönlichkeitsgefährdung durch Zugriff oder Beeinträchtigung seiner Person.¹⁶

¹⁰ Arning/Forgó/Krügel, DuD 2006, 700 (701).

¹¹ Dammann, in: Simitis (Hrsg.), BDSG a.F., 8. Aufl. 2014, § 3 Rn. 31.

¹² Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 273; zum Vorfeldschutz allgemein BVerfGE 118, 168 (184); Grimm, JZ 2013, 585 (586); v. Lewinski, Die Matrix des Datenschutzes, 2014, S. 78 ff.

¹³ BVerfGE 65, 1 (43); Grimm, JZ 2013, 585 (586).

¹⁴ Siehe auch den Beitrag von Jungkunz et al. in diesem Band.

¹⁵ Vgl. BVerfGE 118, 168 (184); Grimm, JZ 2013, 585 (586).

¹⁶ Arning/Forgó/Krügel, DuD 2006, 700 (701); Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 268, 285 f.

2.2 Identifizierbarkeit im Kontext anonymer und pseudonymer Datennutzung

2.2.1 (Faktisch) anonyme Nutzung klinischer Daten zu Forschungszwecken

Erwägungsgrund (EG) 26 DSGVO enthält für Art. 4 Nr. 1 DSGVO weitere konkretisierende Vorgaben für die Identifizierbarkeit. Nach EG 26 S. 5 DSGVO wird dem personenbezogenen Datum das anonyme Datum gegenübergestellt. EG 26 S. 5 DSGVO führt aus, „die Grundsätze des Datenschutzes sollten [...] nicht für anonyme Informationen gelten [...], die sich nicht auf eine identifizierte oder identifizierbare [...] Person beziehen [...]“. Systematisch knüpft das Begriffspaar „identifiziert“ oder „identifizierbar“ in EG 26 S. 5 an EG 26 S. 3 und 4 DSGVO an. Hiernach sind zur Feststellung der Identifizierbarkeit alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden. Dabei sind objektive Faktoren wie die Kosten der Re-Identifizierung und der erforderliche Zeitaufwand einzubeziehen. Der Verordnungsgeber verdeutlicht in EG 26 DSGVO, dass für die Anonymität eines Datums nicht zwingend die Identifizierungsmöglichkeit unumkehrbar aufgehoben werden muss. Vielmehr genügt es, wenn nach allgemeinem Ermessen wahrscheinlich, also nach der allgemeinen Lebenserfahrung im konkreten Einzelfall, kein Mittel zur Re-Identifizierung zur Verfügung steht.¹⁷ Insoweit ist die Rede von „faktischer“ Anonymität in Abgrenzung zur „absoluten“ Anonymität.¹⁸ Auch der nationale Gesetzgeber geht in § 27 Abs. 3 S. 1 BDSG von der Möglichkeit der Anonymisierung auch bei besonderen Kategorien von Daten (z. B. Gesundheitsdaten oder genetischen Daten) aus.¹⁹

Dass die DSGVO faktische Anonymität ausreichen lässt, wirkt sich besonders bei genetischen Daten aus, denen regelmäßig der unverwechselbare Personenbezug immanent ist – man denke etwa an Gensequenzen in ausreichend großer Zahl.²⁰ Auch bei genetischen Daten nach Art. 4 Nr. 13 DSGVO muss (aus der Perspektive des Verantwortlichen) für die Anwendbarkeit der DSGVO zunächst ein personenbezogenes Datum vorliegen.²¹ Der Ausschluss des personenbezogenen Datums kommt bei genetischen Daten regelmäßig nur in

¹⁷ Statt vieler *BfDI*, Positionspapier zur Anonymisierung unter der DSGVO, 2020, S. 4; *Wellbrock*, *MedR* 2003, 77 (78).

¹⁸ *Haase*, *Datenschutzrechtliche Fragen des Personenbezugs*, 2015, S. 307.

¹⁹ Hierauf hinweisend *BfDI*, Positionspapier zur Anonymisierung unter der DSGVO, 2020, S. 3.

²⁰ Untersuchungen zeigen, dass für die Gewährleistung der Einzigartigkeit der Gensequenz eines Individuums bereits etwa acht *Short Tandem Repeats* oder etwa 70 SNP (*Single Nucleotide Polymorphismen*) genügen, vgl. *Fleischer*, *Rechtliche Aspekte der Systemmedizin*, 2018, S. 272 f.; v. *Kalle/Ücker/et al.*, in: *Stiftung Datenschutz* (Hrsg.), *Big Data und E-Health*, 2017, S. 92.

²¹ *Schwartmann/Mühlenbeck*, in: *Schwartmann et al.* (Hrsg.), *DSGVO/BDSG*, 2. Aufl. 2020, Art. 4 Rn. 239.

Form faktischer Anonymität in Betracht.²² Zwar weisen Daten, die sich unverwechselbar auf eine natürliche Person beziehen (wie bei genetischen Daten oder auch den Minuten des Fingerabdrucks), stets einen (eindeutigen) Bezug zu einer natürlichen Person auf. Sie versetzen jedoch die datenverarbeitende Stelle nicht zu jeder Zeit in die Lage, die hinter dem Datum stehende natürliche Person eindeutig zu identifizieren oder ausreichend einzugrenzen, ohne hierfür auf weiteres Referenzwissen angewiesen zu sein.²³ Das Vorliegen von solchem Referenzwissen, über das mittels eines Matching-Verfahrens die genetischen Daten einer bestimmten Person oder überschaubaren Personengruppe zugeordnet werden können, ist auch bei unverwechselbaren Daten zur Bejahung des personenbezogenen Datums erforderlich.²⁴ Freilich kann mit der Zunahme frei zugänglichen Referenzwissens, etwa in Form genealogischer Datenbanken, der Anwendungsbereich faktisch anonymer genetischer Daten künftig abnehmen.²⁵

2.2.2 Pseudonyme Nutzung klinischer Daten zu Forschungszwecken

Von der Sekundärnutzung klinischer Daten profitiert die Forschung in unterschiedlichen Kontexten. Zu nennen sind die nicht-interventionelle klinische Forschung, Forschung zur Qualitätsverbesserung, Public Health Forschung und hier insbesondere epidemiologische Forschung sowie explorative Datennutzung zum Generieren von Hypothesen oder zur Überprüfung der Machbarkeit geplanter Studien.²⁶ Die verschiedenen Forschungskontexte eint, dass sie in Abgrenzung zur individuellen Behandlung auf einen überindividuellen Erkenntnisgewinn ausgerichtet und in der Regel nicht auf die Kenntnis des hinter dem Datum stehenden individuellen Patienten angewiesen sind.²⁷ Gleichzeitig kann die Re-Identifizierungsmöglichkeit des konkreten Patienten aus den klinischen Daten nicht schlichtweg unwiederbringlich für die Forschungsnutzung entfernt werden. Im Behandlungskontext folgt der Erhalt der Identifizierungsmöglichkeit bereits aus der Dokumentationspflicht des § 630f BGB. Deren Sinn und Zweck macht die fortwährende Identifizierbarkeit des Patienten zumindest bei der behandelnden Stelle erforderlich.²⁸ Auch für die (zumindest theoretisch denkbare) Rückmeldung von Zufalls- oder Zusatzbefunden aus der Forschung an den Patienten ist eine fortwährende Identifizierbarkeit

²² Vgl. *Shabani/Marelli*, EMBO Rep 20 (2019), 1 (4).

²³ *Arning/Forgó/Krügel*, DuD 2006, 700 (701); *Deutscher Ethikrat*, Humanbiobanken für die Forschung, Stellungnahme, 2011, S. 11 f.; *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 281; *Malin/Loukides/Benitez et al.*, Hum Genet 130 (2011), 383 (385); *Molnár-Gábor*, in: Taeger (Hrsg.), Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren, 2017, S. 348.

²⁴ *Arning/Forgó/Krügel*, DuD 2006, 700 (701); *Shabani/Marelli*, EMBO Rep 20 (2019), 1 (3).

²⁵ *Fleischer*, Rechtliche Aspekte der Systemmedizin, 2018, S. 269 f.; *Wellbrock*, MedR 2003, 77 (79).

²⁶ Vgl. den Beitrag von *Jungkunz et al.* in diesem Band.

²⁷ *Ringwald*, NJW 1982, 2593 (2594) am Beispiel epidemiologischer Forschung; *Pommerening et al.*, Das TMF-Datenschutzkonzept für medizinische Datensammlungen und Biobanken, 2009, S. 4.

²⁸ BT-Drs. 17/10488, S. 25 f.

erforderlich.²⁹ Schließlich kann für die Forschungsnutzung selbst die fortbestehende Zuordnungsmöglichkeit der Daten zu einem Individuum notwendig sein, etwa um Redundanzen innerhalb verschiedener Datensätze aus unterschiedlichen Quellen und unterschiedlichen Zeiträumen durch korrekte Zuordnung vorzubeugen, im Falle von Langzeitstudien eine fortlaufende Zuordnung neuer Daten zu bereits vorhandenen Daten zu ermöglichen oder im Rahmen sog. „Follow-up-Untersuchungen“ weitere Studien mit den Daten bestimmter Patienten, von denen in der Vergangenheit bereits Daten verwendet wurden, durchzuführen.³⁰

Diese Aspekte machen in der Praxis biomedizinischer Sekundärnutzung den Einsatz informationeller Gewaltenteilung sowie ausreichender, oft mehraktiger Pseudonymisierungsverfahren erforderlich.³¹ Nach Art. 4 Nr. 5 DSGVO ist Pseudonymisierung das Ersetzen von Identifikationsmerkmalen durch ein Kennzeichen und die getrennte Aufbewahrung dieser zusätzlichen Informationen, um die Identifizierung des Betroffenen auszuschließen.³² Die identifizierenden Elemente des Datums, wie der Name, die Adresse oder andere Identifikatoren, werden nicht gelöscht, sondern durch einen Zuordnungsschlüssel ersetzt, der die Wiederherstellung des Personenbezugs ermöglicht.³³ Hierdurch entstehen getrennte Datensätze.³⁴ Die Erstellung und Verwahrung der getrennten Datensätze kann einer Datentreuhandstelle übertragen werden, die das Pseudonym verwaltet und organisatorisch zwischen die

²⁹Vgl. *Nationaler Ethikrat*, Biobanken für die Forschung, 2004, S. 68 f.; *Pommerening et al.*, Das TMF-Datenschutzkonzept für medizinische Datensammlungen und Biobanken, 2009, S. 5.

³⁰*Albrecht*, CR 1986, 92 (100); *Karaalp*, Der Schutz von Patientendaten für die medizinische Forschung in Krankenhäusern, 2016, S. 211; *Krupp/Preissl*, CR 1989, 121 (126); *Mand*, MedR 2005, 565 (568); *Meier*, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, 2003, S. 265; *Schepers/Semler*, in: Müller-Mielitz/Lux (Hrsg.), E-Health-Ökonomie, 2017, S. 230; *Pöttgen*, Medizinische Forschung und Datenschutz, 2009, S. 84; *Pommerening et al.*, Das TMF-Datenschutzkonzept für medizinische Datensammlungen und Biobanken, 2009, S. 5; *Weichert*, ABIDA Gutachten Big Data im Gesundheitsbereich, 2018, S. 192; *Weichert/Krawczak*, GMS Medizinische Informatik, Biometrie und Epidemiologie Vol. 15 (1) 2019, S. 4.

³¹*Fleischer*, Rechtliche Aspekte der Systemmedizin, 2018, S. 275 f.; *Pommerening et al.*, Das TMF-Datenschutzkonzept für medizinische Datensammlungen und Biobanken, 2009, S. 5; *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 15 Rn. 3.

³²*Art.-29-Datenschutzgruppe*, WP 136, 4/2007, S. 21; *Kingreen/Seidel*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 65.

³³*Gola*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 37; *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 5 Rn. 6 f.

³⁴*Meier*, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, 2003, S. 265 f.

datenhaltende und die forschende Stelle geschaltet ist.³⁵ Sofern für die Forscher der Rückgriff auf die konkreten Patienten nötig ist, kann der individuelle Kontakt über die datenhaltende Stelle, vermittelt durch die Datentreuhandstelle, erfolgen.³⁶

EG 26 S. 2 DSGVO stellt klar, dass pseudonymisierte Daten, die durch Heranziehen zusätzlicher Informationen (insbesondere eines Zuordnungsschlüssels) einer natürlichen Person zugeordnet werden können, als personenbezogene Daten anzusehen sind. Art. 25 Abs. 1 DSGVO spricht von der Pseudonymisierung als Beispiel datenschutzfreundlicher Voreinstellung und nach Art. 32 Abs. 1 lit. a DSGVO ist die Pseudonymisierung ein Element technischer und organisatorischer Maßnahmen.³⁷ Hieraus folgt, dass das Datum auch nach der Pseudonymisierung ein personenbezogenes Datum zumindest für die Stelle bleibt, die sowohl über die Identifikationsmerkmale als auch den Zuordnungsschlüssel verfügt.³⁸

Weniger eindeutig ist dieser Befund aus Sicht der Stelle (etwa der Forscher), die ausschließlich pseudonymisierte Daten ohne Zuordnungsschlüssel erhält und nicht über eigene Identifizierungsmittel verfügt.³⁹ Sofern die Forscher ohne den Zuordnungsschlüssel die hinter den klinischen Daten stehende Person nicht mit eigenen Mitteln identifizieren können, ist zu fragen, ob die Pseudonymisierung für die Forscher faktisch anonymisierend wirkt. Andererseits könnte zum umfassenden Schutz der Daten den Forschern das bei der dritten Stelle vorhandene Zusatzwissen (in Form des Zuordnungsschlüssels) wie eigenes Wissen zuzurechnen sein. Diese Zurechnungsfrage hängt davon ab, wie mit dem Zusatzwissen Dritter im Bereich nicht identifizierter, aber identifizierbarer Daten umzugehen ist. Insbesondere im Bereich der Fremdforschung, in der die datenhaltende, die behandelnde und die forschende Stelle keinerlei wechselseitigen organisatorischen Bezug haben, wird diese Zurechnungsfrage relevant.⁴⁰ Wenn dagegen – wie bei der Eigenforschung – die datenerhebende und die forschende Stelle identisch sind, stellt sich die Zurechnungsfrage solange nicht, wie eben diese Stelle auf identifizierendes Zusatzwissen selbst jederzeit zugreifen kann.

³⁵ Pöttgen, Medizinische Forschung und Datenschutz, 2009, S. 89 ff.

³⁶ Vgl. Rüpkе/Lewinski/Eckhardt, Datenschutzrecht, 2018, S. 145.

³⁷ Rüpkе/Lewinski/Eckhardt, Datenschutzrecht, 2018, S. 145.

³⁸ Gola, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 37; Schneider, Sekundärnutzung klinischer Daten, 2015, S. 12.

³⁹ Zum Streit Fleischer, Rechtliche Aspekte der Systemmedizin, 2018, S. 276 ff.

⁴⁰ Vgl. Fleischer, Rechtliche Aspekte der Systemmedizin, 2018, S. 277 f.

2.3 Die Diskussion um die Reichweite des zurechenbaren Zusatzwissens

2.3.1 Objektiver Ansatz

Teile der Literatur⁴¹ und vereinzelte Gerichte⁴² sowie tendenziell die Datenschutzaufsichtsbehörden⁴³ vertreten eine objektive (absolute) Sichtweise. Hiernach genüge für eine ausreichende Anonymisierung und das Entfallen des Personenbezugs nicht allein das Nichtvorhandensein von identifizierendem Zusatzwissen bei der verantwortlichen (forschenden) Stelle. Vielmehr bedürfe es der Beseitigung der Identifikatoren auch bei sonstigen Dritten, bei denen Zusatzwissen vorhanden ist, beispielsweise bei der datenerhebenden, behandelnden Stelle, die diese Identifikatoren zu Dokumentationszwecken speichert.⁴⁴ Demnach wäre es zur Bejahung des personenbezogenen Datums ausreichend, wenn die nach EG 26 S. 3 DSGVO maßgeblichen Mittel für die Identifizierbarkeit bei irgendeiner beliebigen Stelle vorliegen. Irrelevant sei, ob es sich hierbei um die forschende Stelle selbst, eine Datentreuhandstelle oder den behandelnden Arzt handle. Unerheblich sei auch, ob das Zusatzwissen einer privaten Stelle oder einer Behörde zur Verfügung stehe oder ob auf dieses Wissen nur mittels hoheitlicher Maßnahmen oder unter Zuhilfenahme illegaler Mittel zugegriffen werden könne.⁴⁵ Ebenfalls unerheblich sei, ob die betrachtete Stelle – etwa der Forscher, dem pseudonymisierte Daten übermittelt wurden – tatsächlich auf dieses Zusatzwissen (etwa den Zuordnungsschlüssel) zugreifen könne oder nicht.⁴⁶ Ein personenbezogenes Datum liege hiernach absolut und für jedermann vor, wenn eine Identifizierung oder Identifizierbarkeit auch nur für irgendjemanden möglich sei.⁴⁷ Pseudonymisierte Daten wären hiernach bereits deshalb stets und für jedermann personenbezogen, da die Identifizierungsmöglichkeit erhalten bleibt.

⁴¹ Behm, RDV 2010, 61 (63 f.); Dochow, MedR 2019, 279 (284); Härting, ITRB 2016, 36 ff.; Pahlen-Brandt, DuD 2008, 34 ff.; dies., K & R 2008, 286 ff.; in diese Richtung Weichert, ABIDA Gutachten Big Data im Gesundheitsbereich, 2018, S. 141; ders., in: D/W/W/S, EU-DSGVO, 2. Aufl. 2020, Art. 4 Rn. 19.

⁴² Bei dynamischen IP-Adressen AG Berlin-Mitte, K & R 2007, 600 (601); VG Wiesbaden, MMR 2009, 428 (432).

⁴³ AK Medien, Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten, abgedr. im 31. TB des Hessischen DSB, Kap. 2.5.3, dort Kap. 3.1, Abs. 4; Düsseldorfer Kreis, Beschl. der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27.11.2009 in Stralsund, S. 1; ULD Schleswig-Holstein, IP-Adressen und andere Nutzungsdaten – Häufig gestellte Fragen, Ziff. I 1; in diese Richtung wohl auch BfDI, Positionspapier zur Anonymisierung unter der DSGVO, 2020, S. 4.

⁴⁴ Weichert, ABIDA Gutachten Big Data im Gesundheitsbereich, 2018, S. 141.

⁴⁵ Pahlen-Brandt, K & R 2008, 286 (289).

⁴⁶ Pahlen-Brandt, DuD 2008, 34 (38); Weichert, DuD 2007, 113 (115).

⁴⁷ So etwa Pahlen-Brandt, DuD 2008, 34 ff.; dies., K & R 2008, 286 (289).

Für eine objektive Sichtweise soll der hierdurch gewährleistete umfassende Schutz der informationellen Selbstbestimmung sprechen.⁴⁸ Dies entspreche zumindest national auch den Vorgaben des BVerfG im Volkszählungsurteil, wonach es kein belangloses Datum mehr gebe und personenbezogene Daten somit umfassend zu schützen seien.⁴⁹ Zudem könne eine objektive Sichtweise die für das Datenschutzrecht so wichtige Frage nach dem Anwendungsbereich einheitlich beantworten, wodurch Rechtsunsicherheiten ausgeschlossen würden.⁵⁰ Nur eine solche Sichtweise, so die Befürworter, ermögliche eine trennscharfe Abgrenzung zwischen personenbezogenen und anonymen Daten und vermeide unpraktikable und unsichere Einzelfallentscheidungen, die letztlich sowohl zu Lasten der informationellen Selbstbestimmung als auch des kalkulierbaren Risikos gingen.⁵¹

Gegen den objektiven Ansatz wird eingewandt, dass hierdurch der vermeintlich Betroffene schon bei einem nur theoretischen Re-Identifizierungsrisiko unter den weitreichenden Schutz des Datenschutzrechts gestellt werde, was zu einer uferlosen und kaum praktikablen Ausdehnung des Datenschutzrechts führe.⁵² Hierdurch werde das Datenschutzrecht auf einen Zeitpunkt nur theoretischer Identifizierbarkeit des Betroffenen erstreckt, in dem schutzwürdige Belange des Betroffenen noch gar nicht berührt seien.⁵³ Der objektive Ansatz verlagere die datenschutzrechtliche Intention des beschriebenen Vorfeldschutzes zu weit nach vorne, da er Sachverhalte mit umfasse, in denen keinerlei Gefahr einer Identifizierung bestünde.⁵⁴

Zudem führe der objektive Ansatz ebenfalls zu Unbestimmtheit und Rechtsunsicherheit. Nach objektivem Maßstab müsste die verarbeitende Stelle den Standpunkt des Meistwissenden antizipieren und letztlich das gesamte „Weltwissen“ für die Frage nach der Identifizierbarkeit zu Grunde legen.⁵⁵ Da die einzelne Stelle regelmäßig gar nicht wissen könne, ob Zusatzwissen bei Dritten tatsächlich (nach wie vor) existiere, müsse sie aus Sicherheitserwägungen bei vielen Datensätzen schlicht unterstellen, dass es sich um personenbezogene Daten handle.⁵⁶ Der objektive Ansatz stelle sich hierdurch nicht nur als tendenziell wirtschafts-, wissenschafts- und innovationsfeindlich dar.⁵⁷ Er widerspreche auch dem Bestimmtheitsgrundsatz, wonach für den Einzelnen erkennbar sein

⁴⁸ Pahlen-Brandt, K & R 2008, 286 (289); *dies.*, DuD 2008, 34 (38).

⁴⁹ Pahlen-Brandt, DuD 2008, 34 (39).

⁵⁰ Referierend Brink/Eckhardt, ZD 2015, 205 (210).

⁵¹ Forgó/Krügel, MMR 2010, 17 (18); Pahlen-Brandt, DuD 2008, 34 (38).

⁵² LG Berlin, ZD 2013, 618 (619); Brink/Eckhardt, ZD 2015, 205 (207).

⁵³ LG Berlin, ZD 2013, 618 (619).

⁵⁴ Schefzig, K & R 2014, 772 (773).

⁵⁵ Kühling/Klar, NJW 2013, 3611 (3616).

⁵⁶ Meyerdiercks, MMR 2009, 8 (10).

⁵⁷ Brink/Eckhardt, ZD 2015, 205 (206).

müsse, welche rechtlichen Pflichten ihn treffen.⁵⁸ Die betrachtete Stelle müsse selbst ihre datenschutzrechtliche Verantwortlichkeit aufgrund eigener Mittel erkennen können.⁵⁹

2.3.2 Subjektiver Ansatz

Dem objektiven Ansatz steht eine subjektive (relative) Sichtweise gegenüber.⁶⁰ Diese stellt für die Frage nach der Identifizierbarkeit auf die konkret betrachtete Stelle und das ihr zur Verfügung stehende Wissen ab.⁶¹ Man müsse aus der Perspektive der verarbeitenden Stelle fragen, welche Mittel und welches Zusatzwissen ihr konkret zur Verfügung stünden.⁶² Das datenschutzrechtliche Pflichtenprogramm solle erst greifen, wenn die jeweils verantwortliche Stelle faktisch die Möglichkeit zur Herstellung eines Personenbezugs habe.⁶³ Eine rein theoretische Identifizierbarkeit des Betroffenen löse noch nicht das Schutzbedürfnis der informationellen Selbstbestimmung aus.⁶⁴ Die Herstellung des Personenbezugs müsse für die verarbeitende Stelle praktisch möglich sein. Zudem ermögliche eine relative Sichtweise der betrachteten Stelle die eindeutige Bestimmung, ob aus ihrer Sicht ein Personenbezug vorliege oder nicht.⁶⁵

2.3.3 Vermittelnder Ansatz

In der Literatur finden sich vermittelnde Auffassungen und Modifikationen von objektivem und subjektivem Ansatz.⁶⁶ Teils wird argumentiert, die Identifizierung des Betroffenen müsse der verarbeitenden Stelle – hier den Forschern – objektiv möglich und subjektiv von ihnen beabsichtigt sein, damit von einer Identifizierbarkeit aus Sicht

⁵⁸ *Meyerdiercks*, MMR 2009, 8 (11).

⁵⁹ *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 294.

⁶⁰ Zu beachten ist, dass ein streng subjektiver Ansatz, der auch dann ausschließlich auf die verarbeitende Stelle abstellt, wenn sie auf Zusatzwissen Dritter zugreifen kann, nur noch selten vertreten wird, etwa bei *Meyerdiercks*, MMR 2009, 8 (9 ff.).

⁶¹ *Arning/Forgó/Krügel*, DuD 2006, 700 (701 ff.); *Brink/Eckhardt*, ZD 2015, 205 f.; *Eckhardt*, K & R 2007, 602 ff.; *ders.*, K & R 2008, 768 f.; *Gola/Schomerus*, in: Gola et al. (Hrsg.), BDSG a.F., 11. Aufl. 2012, § 3 Rn. 10 f.; *Kroschwald*, ZD 2014, 75 (76); *Kühling/Klar*, NJW 2013, 3611 (3615); *Mand*, MedR 2005, 565 (568); *Meyerdiercks*, MMR 2009, 8 ff.; *Nink/Pohle*, MMR 2015, 563 ff.; *Roßnagel/Scholz*, MMR 2000, 721 (722 f.); *Schefzig*, K & R 2014, 772 (773); *Specht/Müller-Riemenschneider*, ZD 2014, 71 ff.; *AG München*, ZUM-RD 2009, 413 (414); *LG Berlin*, MMR 2007, 799 (801); in diese Richtung tendiert auch die *Art.-29-Datenschutzgruppe*, WP 136, 4/2007, S. 17 f., wonach für Pharmaunternehmen Gesundheitsdaten, die ihnen verschlüsselt übermittelt wurden, mangels Identifizierbarkeit keine personenbezogenen Daten seien.

⁶² *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, Teil C Rn. 278.

⁶³ *Karg*, Datenschutzrechtliche Rahmenbedingungen für die Bereitstellung von Geodaten, Gutachten im Auftrag der GIW-Kommission, 2008, S. 16.

⁶⁴ *LG Berlin*, ZD 2013, 618 (619).

⁶⁵ *Nink/Pohle*, MMR 2015, 563 (566).

⁶⁶ Vgl. *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 298 m. w. N.

der Forscher gesprochen werden könne.⁶⁷ Dies würde bereits ausscheiden, wenn die Forscher den Betroffenen nicht selbst für ihre Forschung identifizieren müssten, sondern dies der datenerhebenden Stelle oder zwischengeschalteten Datentreuhandstelle überlassen würden. Das Zusatzwissen Dritter sei zudem dann nicht den Forschern zuzurechnen, wenn ein Zugriff hierauf rechtswidrig sei.⁶⁸

Mit der Frage der Zurechenbarkeit von Zusatzwissen wurde auch der EuGH in Sachen *Breyer* befasst.⁶⁹ Der EuGH stellte in seinem Urteil darauf ab, ob der Zugriff auf Zusatzwissen für die datenverarbeitende Stelle ein Mittel darstelle, dessen Einsatz vernünftigerweise zu erwarten sei.⁷⁰ Dies sei dann nicht der Fall, wenn die Verknüpfung gesetzlich verboten oder praktisch undurchführbar und das Risiko einer Identifizierung daher faktisch vernachlässigbar sei.⁷¹ Für die Zurechnung von Zusatzwissen Dritter sei daher entscheidend, ob die datenverarbeitende Stelle über rechtliche Mittel verfüge, um auf das Zusatzwissen zuzugreifen.⁷²

Der EuGH folgte in seinem Urteil in weiten Teilen den Schlussanträgen des Generalanwalts *Sánchez-Bordona*, der sich ebenfalls deutlich gegen eine pauschale Einbeziehung des Zusatzwissens Dritter aussprach.⁷³ Aus Sicht des Generalanwalts begründe eine solche objektive Zurechnung die Gefahr, dass faktisch jede Art von Information als personenbezogenes Datum einzuordnen wäre, da die Existenz von Zusatzwissen bei Dritten niemals mit Sicherheit ausgeschlossen werden könne.⁷⁴ Auch seien nur rechtmäßige Mittel in die Beurteilung einzubeziehen, da illegale Mittel nicht mehr als vernünftigerweise erwartbar anzusehen seien.⁷⁵ Der Ansicht des EuGH schloss sich nachfolgend auch der 6. Zivilsenat des BGH an, der dem EuGH die Frage vorgelegt hatte.⁷⁶

2.3.4 Stellungnahme

Das Abstellen des EuGH auf rechtliche Mittel für die Frage nach der Zurechenbarkeit von Zusatzwissen stellt nach hier vertretener Auffassung einen rechtssicheren

⁶⁷ *Buchholtz/Stentzel*, in: Gierschmann et al. (Hrsg.), DS-GVO, 1. Aufl. 2018, Art. 4 Nr. 1 Rn. 12.

⁶⁸ *Buchholtz/Stentzel*, in: Gierschmann et al. (Hrsg.), DS-GVO, 1. Aufl. 2018, Art. 4 Nr. 1 Rn. 12.

⁶⁹ EuGH, ECLI:EU:C:2016:779 – *Breyer*.

⁷⁰ EuGH, ECLI:EU:C:2016:779, Rn. 45 – *Breyer*.

⁷¹ EuGH, ECLI:EU:C:2016:779, Rn. 46 – *Breyer*.

⁷² EuGH, ECLI:EU:C:2016:779, Rn. 49 – *Breyer*; *Bierekhoven*, NJW 2017, 2416 (2420).

⁷³ GA EuGH, ECLI:EU:C:2016:339, Rn. 65 – *Breyer*.

⁷⁴ GA EuGH, ECLI:EU:C:2016:339, Rn. 65 – *Breyer*; *Kühling/Klar*, ZD 2017, 24 (28).

⁷⁵ GA EuGH, ECLI:EU:C:2016:339, Rn. 73 – *Breyer*; *Nink/Pohle*, MMR 2015, 563 (565).

⁷⁶ BGH, NJW 2017, 2416 (2417 f.).

Kompromiss dar.⁷⁷ Der objektive Ansatz ist schon deshalb abzulehnen, weil er in unverhältnismäßiger und damit grundrechtswidriger Weise in Freiheitsgrundrechte eingreift.⁷⁸ Auch die freie Datenverarbeitung ist grundrechtlich geschützt und darf nur mit verhältnismäßigen, also geeigneten, erforderlichen und angemessenen Mitteln beschränkt werden. Zu diesen Freiheitsgrundrechten zählt auch die vorliegend in Rede stehende Wissenschafts- und Forschungsfreiheit (Art. 5 Abs. 3 GG und Art. 13 GRCh).⁷⁹ Die Bejahung des Anwendungsbereichs des Datenschutzrechts zum Schutz personenbezogener Daten greift in rechtfertigungsbedürftiger Weise in die Forschungsfreiheit ein, da hierdurch die Datenverarbeitung als Grundrechtsbetätigung eingeschränkt wird.⁸⁰ Ein verhältnismäßiger Ausgleich zwischen der informationellen Selbstbestimmung der Betroffenen und der Forschungsfreiheit der Forscher, wie ihn das Datenschutzrecht anstrebt, ist bei einem objektiven Ansatz gerade nicht möglich.⁸¹ Faktisch fordert der objektive Ansatz von einer datenverarbeitenden Stelle, vorsorglich alle Informationen als personenbezogene Daten zu behandeln, da irgendeine Stelle auf der Welt über Zusatzwissen verfügen könnte.⁸² Eine solch weitgehende Auslegung der Identifizierbarkeit ist zwar geeignet, einen umfassenden Schutz personenbezogener Daten herzustellen, stellt jedoch nicht das mildeste Mittel für diesen Schutz dar und greift aufgrund seiner Weite unangemessen in entgegenstehende Freiheitsrechte ein. Der datenschutzrechtliche Schutzzweck rechtfertigt zwar ein frühzeitiges Eingreifen des Datenschutzes, fordert aber aus Gründen der Verhältnismäßigkeit ein echtes Gefahrenpotenzial für die Betroffenen.⁸³

Andererseits widerspricht auch ein streng subjektiver Ansatz, der ausschließlich auf den Verantwortlichen abstellt, einem verhältnismäßigen Schutz personenbezogener

⁷⁷ Kühling/Klar, ZD 2017, 24 (28), die jedoch das Erfordernis rechtlicher Mittel relativieren, wenn die faktische Nähe zu den sich bei Dritten befindlichen Daten oder die Sensibilität der Daten, wie z.B. bei klinischen Studien, groß ist und jedenfalls hinreichend konkrete Anhaltspunkte für die Gefahr eines nicht rechtskonformen Zugriffs auf die Daten besteht.

⁷⁸ Brink/Eckhardt, ZD 2015, 205 (210); Schneider, Sekundärnutzung klinischer Daten, 2015, S. 14.

⁷⁹ EU Kommission, Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-GVO), KOM (2012) 11 endg., S. 7; so auch Buchner, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 1 Rn. 15; Roßnagel, ZD 2019, 157 ff.

⁸⁰ Brink/Eckhardt, ZD 2015, 205 (210); Masing, NJW 2012, 2305 (2307).

⁸¹ So auch Brink/Eckhardt, ZD 2015, 205 (210); Buchholtz/Stentzel, in: Gierschmann et al. (Hrsg.), DS-GVO, 1. Aufl. 2018, Art. 4 Rn. 11; Meyerdiercks, MMR 2009, 8 (10).

⁸² Pointiert Buchholtz/Stentzel, in: Gierschmann et al. (Hrsg.), DS-GVO, 1. Aufl. 2018, Art. 4 Nr. 1 Rn. 11.

⁸³ Arning/Rothkegel, in: Taeger/Gabel (Hrsg.), DSGVO-BDSG, Art. 4 Nr. 1 Rn. 36 f.; Buchholtz/Stentzel, in: Gierschmann et al. (Hrsg.), DS-GVO, 1. Aufl. 2018, Art. 4 Nr. 1 Rn. 11; anders wohl VGH Baden-Württemberg, BeckRS 2020, 18980: „das Datenschutzrecht [kennt] kein ‘erlaubtes Risiko‘“.

Daten. Eine solche Sichtweise ist auch kaum mit der DSGVO vereinbar, die wenigstens in EG 26 S. 3 DSGVO auch die Mittel Dritter unter gewissen Umständen einbezieht.⁸⁴

Den Ausgleich widerstreitender Interessen und zugleich ein rechtssicheres und praxisgeeignetes Zurechnungskriterium bietet dagegen der Ansatz des EuGH. Die Betonung des rechtlichen Mittels ermöglicht ein taugliches Kriterium für die Zurechnung von Zusatzwissen. Die Forscher müssen für die Frage der Zurechnung prüfen, ob sie einen rechtlichen Anspruch auf das bei Dritten vorhandene Zusatzwissen haben oder ob ihnen ein möglicher faktischer Zugriff rechtlich untersagt ist. Eine rechtssichere Lösung bei dieser Prüfung kann ein vorbeugender vertraglicher Ausschluss möglicher Zugriffsansprüche bieten (dazu sogleich). Das Wahrscheinlichkeitsurteil, zu dem Art. 4 Nr. 1 DSGVO und EG 26 im Rahmen der Identifizierbarkeit anhalten, darf nicht in unverhältnismäßiger Weise zu einer pauschal zu frühen oder zu späten Datenschutzbejahung führen. Dem entspricht es, wenn das Zusatzwissen Dritter der datenverarbeitenden Stelle nur dann zugerechnet wird, wenn ein Zugriff im Bereich des nach allgemeinem Ermessen Wahrscheinlichen liegt. Dies wiederum ist anzunehmen, wenn rechtliche Zugriffsmittel auf das Zusatzwissen existieren. Andererseits ist das Risiko einer Identifizierung faktisch vernachlässigbar, wenn die Verknüpfung mit Zusatzwissen gesetzlich verboten oder praktisch undurchführbar ist.⁸⁵ Der Ansatz ermöglicht einen ausgewogenen und verhältnismäßigen Ausgleich zwischen dem kollidierenden Schutz potenzieller Betroffener einerseits und freiem Informationsumgang andererseits.⁸⁶ Diesem Ausgleich dient auch das Ausklammern illegaler Mittel im Rahmen der Identifizierbarkeit. Der verarbeitenden Stelle kann nicht pauschal rechtswidriges Handeln bei der Beurteilung der Identifizierbarkeit unterstellt werden, zumal die Rechtsordnung bereits ausreichende Schutzmechanismen zur Abwehr rechtswidrigen Verhaltens implementiert hat, ohne dass ein solches Verhalten fiktiv unterstellt werden müsste.⁸⁷

2.4 Empfang faktisch anonymer Daten bei den Forschern

2.4.1 Konsequenz des vermittelnden Ansatzes

Für die Nutzung pseudonymisierter klinischer Daten in der biomedizinischen Forschung hat der vermittelnde Ansatz zur Folge: Empfangen die Forscher ausschließlich den nicht identifizierenden Teil eines pseudonymisierten Datums ohne Zuordnungsschlüssel und verfügen sie weder über eigenes Zusatzwissen noch über einen rechtlichen Anspruch auf den Schlüssel oder sonstige legale Zugriffsmöglichkeiten, handelt es sich für sie um ein

⁸⁴ *Brink/Eckhardt*, ZD 2015, 205 (209); *Dregelies*, VuR 2017, 256 (257).

⁸⁵ EuGH, ECLI:EU:C:2016:779, Rn. 45 – *Breyer*.

⁸⁶ I. Erg. auch *Kühling/Klar*, ZD 2017, 24 (28).

⁸⁷ Vgl. EuGH, ECLI:EU:C:2016:779, Rn. 45 – *Breyer*; GA EuGH, ECLI:EU:C:2016:339, Rn. 73; a. A. *Weichert*, ABIDA Gutachten Big Data im Gesundheitsbereich, 2018, S. 141.

faktisch anonymes Datum. Die Verarbeitung dieses Datums fällt für die Forscher nicht unter das Datenschutzrecht.⁸⁸ Die Pseudonymisierung hat für die Forscher eine subjektiv anonymisierende Wirkung.⁸⁹

Für die übermittelnde Stelle, die über den Zuordnungsschlüssel verfügt, bleibt das Datum auch nach der Pseudonymisierung ein personenbezogenes Datum. Die Übertragung des pseudonymen Datums von dieser Stelle an die Forscher – obgleich beschränkt auf den subjektiv anonymen Anteil – stellt für die übermittelnden Personen einen rechtfertigungsbedürftigen Datenverarbeitungsvorgang dar.⁹⁰

2.4.2 Kautelarjuristische Handlungsempfehlung

Da der EuGH das Vorhandensein rechtlicher Mittel betont, sollten die Forscher umfassend vertraglich auf die Kenntnisnahme von Zusatzwissen verzichten und sich zudem einem Verbot der Re-Identifizierung unterwerfen.⁹¹ So könnte im Fall der Übermittlung pseudonymisierter Daten von einem behandelnden Arzt an einen Forscher vertraglich geregelt werden, dass der Forscher keinerlei Ansprüche auf den Zuordnungsschlüssel oder sonstiges beim Behandelnden vorhandenes Zusatzwissen über den Betroffenen geltend machen wird, keinerlei Versuch unternimmt, auf das Zusatzwissen zuzugreifen und auch sonst die Daten nicht in einer Weise nutzt, die zur Re-Identifizierung des Betroffenen führen kann.⁹²

Ein solcher vorbeugender vertraglicher Verzicht sollte mit Kontrollen und Sanktionen verbunden werden, die ein vertragswidriges Verhalten unwahrscheinlich machen.⁹³ Die Vereinbarung kann etwa mit einem außerordentlichen Kündigungsrecht und einer angemessen hohen Vertragsstrafe kombiniert werden. Diese vertraglichen Hürden können zu einer nach allgemeinem Ermessen fehlenden Identifizierungswahrscheinlichkeit i. S. d. EG 26 führen.⁹⁴ Hierdurch kann in der Praxis verhindert werden, dass das bei

⁸⁸ So auch Art.-29-Datenschutzgruppe, WP 136, 4/2007, S. 17 f.

⁸⁹ Ziebarth, in: Sydow (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 4 Rn. 98; in diese Richtung Schefzig, K & R 2014, 772 (776 f.).

⁹⁰ Vgl. Roßnagel/Scholz, MMR 2000, 721 (730); anders Schneider, Sekundärnutzung klinischer Daten, 2015, S. 24.

⁹¹ Vgl. Arning/Rothkegel, in: Taeger/Gabel (Hrsg.), DSGVO-BDSG, 3. Aufl. 2019, Art. 4 Rn. 54; Dammann, in: Simitis (Hrsg.), BDSG a.F., 8. Aufl. 2014, § 3 Rn. 31; in diese Richtung auch Brink/Eckhardt, ZD 2015, 205 (211); Forgó/Krügel, MMR 2010, 17 (18); anders Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 303, 305; Fleischer, Rechtliche Aspekte der Systemmedizin, 2018, S. 260.

⁹² Vgl. zu letzterem Punkt DKFZ, Data Transfer Agreement of Human Data for Research Purposes, Klausel 5, www.dkfz.de/en/CanEpi/EGA/Data-Transfer-Agreement-of-Human-Data-for-Research-Purposes-Jan.-2020.pdf (Zugriff: 29.7.2021).

⁹³ Dammann, in: Simitis (Hrsg.), BDSG a.F., 8. Aufl. 2014, § 3 Rn. 31.

⁹⁴ Vgl. Arning/Rothkegel, in: Taeger/Gabel (Hrsg.), DSGVO-BDSG, 3. Aufl. 2019, Art. 4 Rn. 54; Kroschwald, ZD 2014, 75 (76).

der behandelnden, datenerhebenden Stelle vorhandene Zusatzwissen dem Forscher als eigenes Wissen über den Betroffenen zugerechnet wird.

Ein weiterer vertraglicher Aspekt in der Kautelarlösung sollte für den zusätzlichen Schutz der von Forschern empfangenen klinischen Daten beachtet werden: Auch wenn die Daten für die Forscher faktisch anonym sind, behalten sie doch ihren sensiblen Charakter und sind anfällig für Hacker oder Cyber-Attacken durch Außenstehende.⁹⁵ Da jedoch die Forscher aufgrund der für sie anonymen Daten nicht unter das Datenschutzrecht fallen, entfällt für sie zugleich die Pflicht zum Vorhalten technischer und organisatorischer Maßnahmen zum Schutz der Daten nach Art. 24, 32 DSGVO. Daher sollten die datenempfangenden Forscher vertraglich zu einem dem Stand der Technik entsprechenden Schutz der Daten vor unberechtigtem Zugriff und Datenmissbrauch verpflichtet werden.⁹⁶ Ein solcher verlängerter Schutz der Daten bei den Forschern kann wiederum Beachtung im Rahmen des datenschutzrechtlich relevanten Übermittlungsvorgangs vom Behandelnden an die Forscher finden, etwa im Rahmen einer Risikoabwägung gem. Art. 35 (Abs. 3 lit. b) DSGVO. Hierin ist auch kein (unzulässiges) vertragliches Abbedingen der DSGVO zu sehen. Aus der Nichtanwendbarkeit der DSGVO kann nicht geschlossen werden, dass die Daten technisch nicht geschützt werden müssen. Die vertragliche Vereinbarung technischen Schutzes ist zulässiger Ausdruck von Vertragsfreiheit, zumal der technische Schutz von Daten auch außerhalb personenbezogener Daten üblich ist.

2.5 Übertragung faktisch anonymen Daten durch die Forscher

2.5.1 Konsequenz des vermittelnden Ansatzes

Nach Empfang der Daten durch die Forscher stellt sich weiter die Frage, ob die für sie faktisch anonymen Daten an Dritte übertragen oder sogar zur freien Verfügung ins Internet gestellt werden dürfen. Praktisch relevant ist dies, wenn die Forscher Ergebnisse ihrer Forschung und damit zusammenhängend die Datengrundlage mit der Scientific Community teilen möchten.⁹⁷ Da die Daten unter den beschriebenen Voraussetzungen für die Forscher datenschutzrechtlich frei nutzbar sind, können sie diese Daten grundsätzlich auch frei von datenschutzrechtlicher Restriktion an Dritte weitergeben. Denkbar ist beispielsweise, dass eine Forschergruppe die aus ihrer Sicht faktisch anonymen

⁹⁵ Hierzu Jäschke/Lingen, in: Jäschke (Hrsg.), Datenschutz im Gesundheitswesen, 2. Aufl. 2018, S. 146.

⁹⁶ Zur vertraglichen Verpflichtung zu technischen Schutzvorkehrungen: DKFZ, Data Transfer Agreement of Human Data for Research Purposes, Klausel 5, www.dkfz.de/en/CanEpi/EGA/Data-Transfer-Agreement-of-Human-Data-for-Research-Purposes-Jan.-2020.pdf (Zugriff: 29.7.2021).

⁹⁷ Schaar, ZD 2016, 224 (226); Weichert, ZD 2020, 18 (20).

Daten einem Pharmaunternehmen zur weitergehenden Nutzung zur Verfügung stellen möchte.⁹⁸

Auf den ersten Blick ist die datenschutzrechtlich unbeschränkte Möglichkeit der Übertragung von der forschenden Stelle an das Pharmaunternehmen konsequente Folge des vermittelnden Ansatzes. Ein etwaiges Korrekturbedürfnis dieser Situation könnte mit dem Argument abgelehnt werden, dass zumindest das Pharmaunternehmen, das die Daten empfängt und über Zusatzwissen oder Zusatzmittel für eine mögliche Re-Identifizierung (etwa aufgrund der eigenen Zugriffsmöglichkeit auf einen Referenzdatenbestand oder der Nutzungsmöglichkeit leistungsstarker Rechenzentren) verfügt, datenschutzrechtlich verantwortlich ist und einer Rechtsgrundlage zum Erheben und Speichern der Daten bedarf.⁹⁹ Diese Annahme würde jedoch dem Gedanken des datenschutzrechtlichen Vorfeldschutzes bei der Identifizierbarkeit (s.o.) und der allgemeinen Risikoverantwortung der übertragenden Stelle widersprechen. Die übertragende Forschergruppe setzt mit der Übertragung der Daten an das Pharmaunternehmen eine Ursache für eine erhöhte Gefährdung durch Re-Identifizierung des Betroffenen. Zudem weist die Annahme Lücken bei der Drittlandübertragung auf, wenn der Empfänger nach Art. 3 DSGVO nicht unter die DSGVO fällt.¹⁰⁰ Deshalb ist die Situation der freien Übertragbarkeit der Daten durch die Forschergruppe korrekturbedürftig.

Von der Literatur wird teilweise eine Korrektur in Form der Zurechnung von Zusatzwissen bejaht, wenn eine Stelle die für sie faktisch anonymen Daten an eine andere Stelle überträgt, die über Zusatzwissen oder Zusatzmittel verfügt.¹⁰¹ Hiernach bräuchte die Forschergruppe für die Übertragung von für sie faktisch anonymen Daten an das Pharmaunternehmen aufgrund des dort vorhandenen Referenzdatenbestands oder des Zugriffs auf leistungsstarke Rechenzentren und der damit einhergehenden Re-Identifizierungsmöglichkeit eine datenschutzrechtliche Rechtsgrundlage. Gleiches würde gelten, wenn die Forschergruppe die für sie faktisch anonymen Daten zur freien Verfügung ins Internet hochladen würde, da hierdurch die Wahrscheinlichkeit, dass irgendeine zugriffnehmende Stelle über Zusatzwissen für eine mögliche Re-Identifizierung verfügt, erheblich gesteigert würde. Obwohl das Datum für die übertragende Forschergruppe zunächst faktisch anonym ist, handelt es sich nun aufgrund des Wissens oder der Mittel der empfangenden Stelle rückwirkend um eine datenschutzrechtlich relevante Übermittlung.¹⁰² Gestützt wird diese Fiktion auf EG 26 S. 3 DSGVO, der die

⁹⁸ Zu einem ähnlichen Beispiel vgl. *Art.-29-Datenschutzgruppe*, WP 136, 4/2007, S. 18.

⁹⁹ Eine Schutzlücke deshalb bezweifelnd *Eckhardt*, K & R 2007, 602 (603).

¹⁰⁰ Vgl. den Beitrag von *Schrader* in diesem Band.

¹⁰¹ *Brink/Eckhardt*, ZD 2015, 205 (211); *Dammann*, in: Simitis (Hrsg.), BDSG a.F., 8. Aufl. 2014, § 3 Rn. 26; *Gola/Schomerus*, in: Gola et al. (Hrsg.), BDSG a.F., 11. Aufl. 2012, § 3 Rn. 10, 44a; *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 Rn. 27; *Kühling/Klar*, NJW 2013, 3611 (3615).

¹⁰² Von „rückwirkend“ spricht etwa der GA EuGH, ECLI:EU:C:2016:339, Rn. 77 – *Breyer*.

Mittel anderer Personen mit einbezieht. Das Wissen Dritter müsse zumindest dann in die Bewertung des Personenbezugs eingestellt werden, wenn der Dritte mit den fraglichen Daten in Berührung komme, etwa indem sie ihm übermittelt oder sonst zur eigenen Verfügung gestellt würden.¹⁰³ Auch wenn der Zurechnung von Zusatzwissen in solchen Übertragungssituationen zuzustimmen ist, sind weitere Ergänzungen nötig:

Zunächst erscheint es unstimmig, von einer Rückwirkung des Personenbezugs ab dem Zeitpunkt des Datenempfangs zu sprechen. Eine Fiktion mit *ex tunc*-Wirkung ist zwar rechtlich denkbar, jedoch weder gesetzlich angedeutet noch zielführend für die nähere Bestimmung der Reichweite der Zurechnungswirkung. Stattdessen sollte von einer „Vorwirkung“ des Zusatzwissens des Dritten im Moment der Datenübermittlung gesprochen werden. Diese Vorwirkung bewirkt eine veränderte Sichtweise, die nicht den Empfang als auf die Übermittlung rückwirkendes Ereignis, sondern den Übermittlungszeitpunkt betont.¹⁰⁴ Im Zeitpunkt der Übertragung der für die Forschergruppe faktisch anonymen Daten muss sie sich daher die Frage stellen, ob das empfangende Pharmaunternehmen über etwaiges Zusatzwissen zur Re-Identifizierung des Betroffenen verfügt. Sofern sie diese Frage nach allgemeinem Ermessen wahrscheinlich bejahen muss, benötigt die Forschergruppe für die Übertragung eine datenschutzrechtlichen Rechtsgrundlage, obwohl die Daten für sie grundsätzlich faktisch anonym und daher datenschutzrechtlich frei verfügbar sind.

Diese Ergänzung beschränkt auch die oben beschriebene Zurechnungswirkung. Zunächst wird deutlich, dass es für die Beurteilung des beim Empfänger vorhandenen Zusatzwissens entscheidend auf den Übertragungszeitpunkt ankommt. Zusatzwissen oder Zusatzmittel, die der Empfänger erst nach der Übertragung des Datums erwirbt oder gar Folgeübermittlungen des Dritten an Dritte, sind nicht mehr von der Zurechnung umfasst.¹⁰⁵ Die Vorwirkung im Zeitpunkt der Übertragung verdeutlicht, dass die Zurechnung des Zusatzwissens auf den konkreten Übertragungsvorgang beschränkt bleibt. Sofern sich nichts an der faktischen Anonymität der Daten bei der Forschergruppe ändert, ist sie somit außerhalb der Übertragung an das besagte Pharmaunternehmen frei von datenschutzrechtlicher Bindung.

Schließlich konkretisiert der Gedanke der Vorwirkung den bei der Forschergruppe zu fordernden Grad der Kenntnis bezüglich des beim Pharmaunternehmen vorhandenen Zusatzwissens. Teilweise wurde hier vertreten, dass die übertragende Stelle stets und

¹⁰³ *Dammann*, in: Simitis (Hrsg.), BDSG a.F., 8. Aufl. 2014, § 3 Rn. 19; *Gola/Schomerus*, in: Gola et al. (Hrsg.), BDSG a.F., 11. Aufl. 2012, § 3 Rn. 10, 44a; *Kühling/Klar*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 Rn. 26.

¹⁰⁴ *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 Rn. 24.

¹⁰⁵ Anders dagegen *Dammann*, in: Simitis (Hrsg.), BDSG a.F., 8. Aufl. 2014, Art. 4 Nr. 1 Rn. 38, der auch später hinzutretendes Zusatzwissen und Folgeübermittlungen in die Zurechnung einbeziehen will und damit das datenschutzrechtliche Haftungsrisiko für die übermittelnde Stelle unkontrollierbar ausdehnt; krit. hierzu *Bergt*, ZD 2015, 365 (369).

verdachtsunabhängig die gegenwärtigen und künftigen Re-Identifizierungsmöglichkeiten der empfangenden Stelle zu evaluieren habe.¹⁰⁶ Eine solche pauschale Prüfungspflicht stünde jedoch in der Nähe des für unverhältnismäßig erachteten objektiven Ansatzes in der Übertragungssituation.¹⁰⁷ Der Übertragende weiß in der Regel nicht, über welches Wissen der Datenempfänger verfügt oder künftig verfügen wird. Er müsste daher sicherheitshalber vom Vorhandensein von Zusatzwissen ausgehen.

Überzeugender ist daher, auf positive Kenntnis des Übertragenden oder zumindest die Erkennbarkeit des nach allgemeinem Ermessen wahrscheinlichen Zusatzwissens bei der empfangenden Stelle abzustellen.¹⁰⁸ Nur wenn die übertragende Forschergruppe im Übertragungszeitpunkt damit rechnen muss, dass dem Pharmaunternehmen nach allgemeinem Ermessen wahrscheinlich (EG 26 S. 3 DSGVO) Zusatzwissen für eine mögliche Re-Identifizierung zur Verfügung steht, ist der Forschergruppe dieses Wissen zuzurechnen. Mit solchem vorhandenem Zusatzwissen muss die Forschergruppe insbesondere dann rechnen, wenn sie die Daten frei zugänglich ins Internet stellt, da hier das Vorhandensein von Zusatzwissen bei irgendeiner zugreifenden Stelle nach allgemeinem Ermessen zu erwarten ist.¹⁰⁹

2.5.2 Kautelarjuristische Handlungsempfehlung

In der Praxis kann es sich aus Gründen der Rechtssicherheit auch in der Übertragungssituation für die verantwortliche Forschungseinrichtung anbieten, mit dem Dritten, dem sie Daten übertragen möchte, eine vertragliche Vereinbarung zu treffen. In einer solchen Vereinbarung sollte die empfangende Stelle der übertragenden Einrichtung zusichern, dass sie über keinerlei Zusatzwissen oder Zusatzmittel zur Identifikation verfügt und auch künftig nicht erwerben oder nutzen wird, um den Betroffenen zu re-identifizieren.¹¹⁰ Auch diese Kautelarpraxis sollte mit einer Vertragsstrafe und einem außerordentlichen Kündigungsrecht für den Fall der Vertragsverletzung abgesichert werden.¹¹¹

¹⁰⁶ Dammann, in: Simitis, BDSG a.F., 8. Aufl. 2014, § 3 Rn. 32; Gola/Schomerus, in: Gola et al. (Hrsg.), BDSG a.F., 11. Aufl. 2012, § 3 Rn. 44a; Kühling/Klar, NJW 2013, 3611 (3615).

¹⁰⁷ Hierauf hinweisend Bergt, ZD 2015, 365 (369); dies ebenfalls konzedierend Dammann, in: Simitis (Hrsg.), BDSG a.F., 8. Aufl. 2014, § 3 Rn. 32.

¹⁰⁸ Gola, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 18 f.; Brink/Eckhardt, ZD 2015, 205 (211).

¹⁰⁹ Klar/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 Rn. 27.

¹¹⁰ Vgl. DKFZ, Data Transfer Agreement of Human Data for Research Purposes, Klausel 5, www.dkfz.de/en/CanEpi/EGA/Data-Transfer-Agreement-of-Human-Data-for-Research-Purposes-Jan.-2020.pdf (Zugriff: 29.7.2021).

¹¹¹ Vgl. DKFZ, Data Transfer Agreement of Human Data for Research Purposes, Klausel 11, www.dkfz.de/en/CanEpi/EGA/Data-Transfer-Agreement-of-Human-Data-for-Research-Purposes-Jan.-2020.pdf (Zugriff: 29.7.2021).

3 Ergebnis

Bevor im Kontext der Sekundärnutzung klinischer Daten zu Forschungszwecken die allgemeinen und bereichsspezifischen datenschutzrechtlichen Rechte und Pflichten diskutiert werden, ist zunächst die Anwendbarkeit des Datenschutzrechts in den Blick zu nehmen. Dabei sollte der Spielraum, der sich zum Schutz des Betroffenen einerseits und zum Erhalt einer effektiven und rechtssicheren Forschungspraxis andererseits bietet, genutzt werden. Hier ist das vom EuGH im Rahmen der Identifizierbarkeit betonte rechtliche Mittel, das den Zugriff auf Wissen zur Bestimmung des Betroffenen erlaubt, entscheidend. Sofern die Forscher klinische Daten zu sekundären Forschungszwecken erhalten, sollte mittels vertraglicher Vereinbarung ein Ausschluss denkbarer rechtlicher Zugriffsmittel auf identifizierendes Zusatzwissen vorgenommen und ein Verbot sonstiger Re-Identifizierungsmaßnahmen vereinbart werden.

Hierdurch kann von der Pseudonymisierung und/oder der Zwischenschaltung von Datentreuhändern eine faktisch anonymisierende Wirkung für die Forscher ausgehen. Voraussetzung ist, dass die Forscher den Betroffenen nicht aufgrund eigenen Wissens oder eigener Mittel re-identifizieren können.¹¹² Das eigene Wissen und die eigenen Mittel müssen die verarbeitenden Forscher unter Berücksichtigung objektiver Faktoren (EG 26 S. 4 DSGVO) sorgfältig und unter etwaiger Einbeziehung der Datenschutzbehörden bewerten, ohne vorschnell eine aus ihrer Sicht vorhandene hinreichende Anonymisierung anzunehmen.¹¹³ Nur unter diesen Voraussetzungen kann sich eine hinreichende Pseudonymisierung als subjektive und somit faktische Anonymisierung im datenschutzrechtlichen Sinne für die Forscher darstellen.

Die genannten Grundsätze gelten auch im Bereich von Sozialdaten, die zu sekundären Forschungszwecken genutzt werden sollen. Nach § 67 Abs. 2 SGB X sind Sozialdaten personenbezogene Daten gem. Art. 4 Nr. 1 DSGVO, die von den sozialrechtlichen Leistungsträgern (insbesondere den gesetzlichen Krankenkassen) zur Erfüllung ihrer Aufgaben verarbeitet werden, sodass auf die datenschutzrechtlichen Ausführungen verwiesen werden kann.

Trotz vertraglicher Gestaltungsmöglichkeiten müssen die datenempfangenden Forscher gerade aufgrund zunehmender Verknüpfungsmöglichkeiten fortwährend kritisch prüfen, ob mit den ihnen zur Verfügung stehenden Mitteln tatsächlich der Betroffene nicht identifiziert werden kann. Es bleibt die Aufgabe und Pflicht jeder präsumtiv verantwortlichen Stelle, die eigenen rechtlichen und tatsächlichen Möglichkeiten einer Re-Identifizierung stets zu evaluieren.

¹¹²Arning/Forgó/Krügel, DuD 2006, 700 (702); Mand, MedR 2005, 565 (568); Ziebarth, in: Sydow (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 4 Rn. 96.

¹¹³Vgl. BfDI, Positionspapier zur Anonymisierung unter der DSGVO, 2020, S. 4.

Danksagung Dieser Beitrag wurde im Rahmen des DFG-geförderten Projekts „Learning from Clinical Data (LinCDat)“ erstellt. Wir möchten uns bei unseren Projektpartner*innen Prof. Dr. Eva Winkler, Dr. Christoph Schickhardt, Dr. Katja Mehlis, Anja Köngeter und Dr. Martin Jungkunz bedanken. Ebenso danken wir Amelie Hotz für ihre Unterstützung bei der Recherche zu diesem Beitrag. Schließlich möchten wir den Herausgeber*innen für ihr wertvolles Feedback und die Aufnahme in diesem Sammelband danken.

Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) – 406103282

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.