Stefan Onur Seddig

Chancen und Risiken der Anonymisierung für die Forschung und Wissenschaft aus Sicht des Datenschutzrechts

Übersicht*

Einleitung

Ein wesentliches Ziel der DSGVO ist es, Datenschutz bereits durch Technikgestaltung zu erreichen. In diesem Zusammenhang wird insbesondere die Anonymisierung von personenbezogenen Daten als Patentlösung angesehen. Dabei gestaltet sich die rechtliche Bewertung der Anonymisierung als zweischneidig. Auf der einen Seite ist sie als eine datenschutzfreundliche technische und organisatorische Maßnahme einzuordnen, da die im Folgeschritt erlangten anonymisierten Daten den Anwendungsbereich der DSGVO grundsätzlich ausschließen. Auf der anderen Seite verlangt das sogenannte Verbotsprinzip für jeden Vorgang, der unter den Begriff der Verarbeitung in Art. 4 Nr. 2 DSGVO fällt, eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO. Sofern die Anonymisierung von Daten als eine Verarbeitung anzusehen ist, gehört sie folgerichtig auch in den Anwendungsbereich des Datenschutzrechts. Der Schutzzweck der DSGVO – unter anderem der Schutz des Datenschutzgrundrechtes – ist durch anonyme Daten jedoch gerade nicht betroffen. Vor diesem Hintergrund gilt es zunächst zu klären, ab wann im rechtlichen Sinne anonyme bzw. anonymisierte Daten vorliegen und ob der Vorgang der Anonymisierung tatsächlich unter das Verbotsprinzip fällt. Daran schließt sich die Problematik an, welche Erlaubnistatbestände, insbesondere im Hinblick auf die verschärften Anforderungen für die Verarbeitung besonderer Kategorien personenbezogener Daten wie Gesundheitsdaten gem. Art. 9 Abs. 1 DSGVO, den Vorgang legitimieren können. Darüber hinaus beantwortet dieser Beitrag die zentrale Frage, ob eine Anonymisierung personenbezogener Daten auch ohne Einwilligung der betroffenen Person rechtlich zulässig ist und welche Chancen sich für Forschung und Wissenschaft daraus ergeben. Abschließend wird erörtert, ob und welche Schutzmaßnahmen für anonymisierte Daten existieren und inwiefern die Pseudonymisierung als bessere Alternative zur Anonymisierung in Betracht gezogen werden kann.

I. Begriffsbestimmung

Zentral für die Bewertung der Anonymisierung und Erörterung der aufgeworfenen datenschutzrechtlichen Fragestellungen ist die Bestimmung der relevanten Begriffe. Dabei ist nicht nur zu bestimmen, was unter Anonymisierung verstanden wird, sondern es muss vor allem auch geklärt werden, ab welchem Punkt im rechtlichen Sinne von anonymen bzw. anonymisierten Daten gesprochen werden kann. Insbesondere ist es angesichts des Fortschritts im Bereich der künstlichen Intelligenz

* Mit Dank an Prof. Dr. Silja Vöneky, Daniel Becker und Nora Hertz für ihre wertvollen Anmerkungen.

(KI) und Big Data fraglich, ob tatsächlich nicht re-individualisierbare Daten erzeugt werden können.

1. Personenbezogene Daten

Unter den Anwendungsbereich der DSGVO[1] fallen ausschließlich personenbezogene Daten. Personenbezogenen Daten werden in Art. 4 Nr. 1 DSGVO legal definiert. Danach sind personenbezogene Daten

> *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, […] identifiziert werden kann."*

Systematisch knüpft das Begriffspaar „identifiziert" oder „identifizierbar" in Erwägungsgrund (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 Identifikation der natürlichen Person genutzt werden.

Problematisch erscheint die Einordung der Reichweite der Identifizierbarkeit.[2] Hierzu bildeten sich in Literatur und Praxis im Grunde zwei Ansätze, der objektive und der subjektive Ansatz heraus. Der objektive Ansatz wird von Teilen der Literatur[3] und einzelnen Gerichte[4] sowie dem Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI)[5] vertreten. Danach entfalle der Personenbezug des Datums nur, wenn weder bei der verantwortlichen Stelle noch bei einer sonstigen dritten Stelle identifizierendes Zusatzwissen vorhanden ist.[6] Folglich würde ein personenbezogenes Datum vorliegen, wenn die nach EG 26 S. 3 DSGVO maßgeblichen Mittel für die Identifizierbarkeit bei irgendeiner beliebigen Stelle vorliegen.[7] Mithin ist nach diesem Ansatz unerheblich, ob es sich hierbei um die verantwortliche bzw. forschende Stelle selbst, eine Datentreuhandstelle, den behandelnden Arzt oder eine Dritte Stelle handele.[8] Schließlich sei auch irrelevant, ob die verantwortliche Stelle tatsächlich auf die Identifikatoren wie bspw. Zuordnungsschlüssel zugreifen kann, welches Interesse die Stelle hat oder ob das Zusatzwissen auf illegalem Wege erhalten wurde.[9] Für die Verfügbarkeit des Zusatzwissens genüge allein die theoretische Möglichkeit.[10]

Der objektive Ansatz wird damit begründet, dass dadurch der umfassende Schutz des Rechts auf informationelle Selbstbestimmung gewährleistet wird.[11] Dieser Ansatz ermögliche eine trennscharfe Abgrenzung zwischen personenbezogenen und anonymen Daten.[12] Demnach vermeide der objektive Ansatz in der Praxis inadäquate Einzelfallentscheidungen.[13] Ferner führt *Pahlen-Brandt* an, dass dieser Ansatz national auch den Vorgaben des Bundesverfassungsgerichtes im Volkszählungsurteil[14] entspreche, wonach es kein belangloses Datum mehr gebe und personenbezogene Daten somit umfassend zu schützen seien.[15] Insgesamt schaffe der objektive Ansatz Rechtssicherheit, indem er die für das Datenschutzrecht so wichtige Frage nach dem Anwendungsbereich einheitlich beantworte.[16]

Gegen diese Ansicht ist vor allem anzuführen, dass der objektive Ansatz in unverhältnismäßiger Weise in

1 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.

2 Ausführlich *Arning/Rothkegel*, in: Taeger/Gabel (Hrsg.), DSGVO – BDSG (2022), 4. Auflage, Art. 4 DSGVO, Rn. 30 ff.; *Spitz/Cornelius*, in: Richter et al. (Hrsg.), Datenreiche Medizin und das Problem der Einwilligung, Personenbezogene Daten im Kontext biomedizinischer Sekundärforschung (2022), 101 (108 ff.); *Bergt*, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts - Überblick über den Theorienstreit und Lösungsvorschlag, ZD (2015), 365-370.

3 *Weichert*, ABIDA Gutachten Big Data im Gesundheitsbereich (2018), 141, abrufbar unter https://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf (zuletzt abgerufen am 08.12.2022); *Forgó/Dügel,* Der Personenbezug von Geodaten - Cui bono, wenn alles bestimmbar ist, MMR (2010), 17 (18); *Behm*, Scoringverfahren unter Einbeziehung von Geodaten, RDV (2010), 61 (63 f.); *Pahlen-Brandt*, Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um „personenbezogene Daten", DuD (2008), 34 (39).

4 VG Wiesbaden, 27.02.2009 - 6 K 1045/08.WI, MMR (2009), 428 (432); AG Berlin-Mitte, 27.03.2007 - 5 C 314/06, K & R (2007), 600 (601).

5 So vgl. BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 29.06.2020, 4; abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf;jsessionid=D6D6B6BAAA504EF283160B8590939B53.intranet231?__blob=publicationFile&v=4 (zuletzt abgerufen am 08.12.2022).

6 *Weichert*, (Fn. 3), 141; *Behm*, (Fn. 3), 61 (63 f.); *Forgó/Dügel,* (Fn. 3), 17 (18).

7 So auch *Spitz/Cornelius*, (Fn. 2), 101 (108).

8 *Spitz/Cornelius*, (Fn. 2), 101 (108); *Weichert*, (Fn. 3), 141.

9 *Weichert*, (Fn. 3), 141; *Bergt*, (Fn. 2), 365 (368 f.).

10 *Weichert*, (Fn. 3), 141.

11 *Pahlen-Brandt*, Zur Personenbezogenheit von IP-Adressen, K & R (2008), 286 (289); vgl. *Forgó/Dügel,* (Fn. 3), 17 (18).

12 *Pahlen-Brandt*, (Fn. 3), 34 (38); vgl. *Forgó/Dügel,* (Fn. 3), 17 (18).

13 *Forgó/Dügel,* (Fn. 3), 17 (18).

14 BVerfG, 15.12.1983 - 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, NJW (1984), 419.

15 *Pahlen-Brandt*, (Fn. 3), 34 (39).

16 *Brink/Eckhardt*, Wann ist ein Datum ein personenbezogenes Datum?, ZD (2015), 205 (210).

Freiheitsgrundrechte eingreift.[17] Diese extensive Auslegung des Anwendungsbereichs des Datenschutzrechts zum Schutz personenbezogener Daten greift in rechtfertigungsbedürftiger Weise insbesondere in die Forschungsfreiheit ein, da hierdurch die Datenverarbeitung als Grundrechtsbetätigung eingeschränkt wird.[18] Es kann nämlich zu keinem verhältnismäßigen Ausgleich zwischen der informationellen Selbstbestimmung der betroffenen Person und der Forschungsfreiheit der Forschenden, wie ihn das Datenschutzrecht anstrebt, kommen.[19] Aus dem Grunde, dass der objektive Ansatz einseitig von der verantwortlichen Stelle fordert, vorsorglich alle Informationen als personenbezogene Daten zu behandeln, da irgendeine Stelle über Zusatzwissen verfügen könnte.[20] Dies stellt eine unverhältnismäßige Hürde für unter anderem Forschende dar, die oftmals kein Wissen oder Einblick darüber haben, ob identifizierendes Zusatzwissen bei Dritten existiert.[21] Mithin schafft der objektive Ansatz durch praktisch schwerlich umsetzbare Anforderungen Rechtsunsicherheit.[22] Die strikte Anwendung des objektiven Ansatzes würde im Ergebnis zur Unmöglichkeit der Anonymisierung führen, da die Identifizierbarkeit nicht rechtssicher ausgeschlossen werden könnte.[23] Damit wäre ein im Grunde datenschutzfreundliches Instrument nicht anwendbar.

Diesem objektiven Ansatz wird der subjektive Ansatz entgegengesetzt.[24] Danach hänge die Identifizierbarkeit von der konkret verantwortlichen Stelle und ihrer Kenntnisnahmemöglichkeiten ab.[25] Somit erfolgt beim subjektiven Ansatz aus der Perspektive der verantwortliche Stelle die Beurteilung darüber, welche Mittel und welches Zusatzwissen ihr konkret zur Verfügung stünden.[26] Erst wenn die jeweils verantwortliche Stelle faktisch die Möglichkeit zur Herstellung eines Personenbezugs habe, sollten die Pflichten der DSGVO eingreifen.[27] Über den subjektiven Ansatz könne laut Nink/Pohle die verantwortliche Stelle eindeutig bestimmen, ob aus ihrer Sicht ein Personenbezug vorliege oder nicht.[28] Dieser Ansatz gewährleiste mehr Rechtssicherheit, da es auch keine Schutzlücken für die betroffene Person gebe.[29]

Vor diesem Hintergrund ist für die Einstufung eines Datums als personenbezogen zentral, wer im konkreten Einzelfall als Verantwortlicher zu qualifizieren ist. Der Verantwortlichkeitsbegriff wird in Art. 4 Nr. 7 DSGVO legaldefiniert.[30] Beispielweise ist für die Einstufung des Verantwortlichen in der Forschung entscheidend, für wen die Forschenden im Einzelfall tätig sind. Wenn die Forschenden an der Universität tätig sind oder für ein Unternehmen tätig sind, dann ist im Regelfall die Universität bzw. das Unternehmen i.S.v. Art. 4 Nr. 7 DSGVO die Verantwortliche.[31] Folglich ist ausgehend von dem zur Verfügung stehenden Wissen und den Ressourcen des Verantwortlichen für jedes Datum zu prüfen, ob es als personenbezogenes Datum zu qualifizieren ist.[32]

Die strikte Anwendung des subjektiven Ansatzes, der ausschließlich auf die verantwortliche Stelle abstellt, führt jedoch nicht automatisch auch zu einem verhältnismäßigen Schutz der personenbezogenen Daten.[33] Der EG 26 S. 3 DSGVO deutet an, dass unter Umständen auf die Mittel Dritter abgestellt werden muss. Somit ist eine

17 Ausführlich *Brink/Eckhardt*, (Fn. 16), 205 (210).

18 *Spitz/Cornelius*, (Fn. 2), 101 (112); *Brink/Eckhardt*, (Fn. 16), 205 (210).

19 *Spitz/Cornelius*, (Fn. 2), 101 (112); *Buchholtz/Stentzel*, in: Gierschmann et al. (Hrsg.), DS-GVO (2018), 1. Aufl., Art. 4 Nr. 1, Rn. 11; *Brink/Eckhardt*, (Fn. 16), 205 (210).

20 *Spitz/Cornelius*, (Fn. 2), 101 (109); *Brink/Eckhardt*, (Fn. 16), 205 (210); *Bergt*, (Fn. 2), 365 (369).

21 Vgl. *Arning/Rothkegel*, (Fn. 2), Rn. 35; *Brink/Eckhardt*, (Fn. 16), 205 (210).

22 Vgl. *Spitz/Cornelius*, (Fn. 2), 101 (109); *Schwartmann/Mühlenbeck*, in: Schwartmann et al. (Hrsg.), DS-GVO/BDSG (2020), 2. Auflage, Art. 4, Rn. 38; *Brink/Eckhardt*, (Fn. 16), 205 (210).

23 So auch *Arning/Rothkegel*, (Fn. 2), Rn. 35; *Schwartmann/Mühlenbeck*, (Fn. 22), Rn. 38.

24 Siehe dazu *Arning/Rothkegel*, (Fn. 2), Rn. 34 f.; *Eßer*, in: Auernhammer (Hrsg.), DSGVO BDSG (2020), 7. Auflage, Art. 4, Rn. 20; *Schwartmann/Mühlenbeck*, (Fn. 22), Rn. 35 ff.; *Nink/Pohle*, Die Bestimmbarkeit des Personenbezugs, MMR (2015), 563 ff.

25 *Arning/Rothkegel*, (Fn. 2), Rn. 34; *Eßer*, (Fn. 24), Rn. 20.

26 *Spitz/Cornelius*, (Fn. 2), 101 (110); vgl. *Schwartmann/Mühlenbeck*, (Fn. 22), Rn. 35.

27 *Spitz/Cornelius*, (Fn. 2), 101 (110).

28 *Nink/Pohle*, (Fn. 24), 563 (566).

29 Ebd.

30 Danach ist „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

31 *Jung/Hansch*, Die Verantwortlichkeit in der DS-GVO und ihre praktischen Auswirkungen, ZD (2019), 143 (143); *Becker*, Die Wissenschaftsprivilegierung der DS-GVO, OdW (2022), 103 (105).

32 *Becker*, (Fn. 31), 103 (105).

33 So auch *Spitz/Cornelius*, (Fn. 2), 101 (113); *Brink/Eckhardt*, (Fn. 16), 205 (209).

ausschließlich losgelöste subjektive Betrachtung nicht vereinbar mit Zielsetzung und Zweck der DSGVO.

Vielmehr braucht es einen Mittelweg, welcher bestimmte Aspekte des objektiven und subjektiven Ansatzes kombiniert[34] Nach einer vermittelnden Ansicht von *Buchholtz/Stentzel* müsse die Identifikation der betroffenen Person der verantwortlichen Stelle objektiv möglich und subjektiv von ihr beabsichtigt sein.[35] Im Forschungskontext würde eine Identifizierbarkeit nach dieser Ansicht dann ausscheiden, wenn die Forschenden die betroffene Person nicht selbst für ihre Forschung identifizieren müssten, sondern dies der datenerhebenden Stelle oder zwischengeschalteten Datentreuhandstelle überlassen würden.[36] Nach *Buchholtz/Stentzel* sei das Zusatzwissen Dritter zudem dann nicht den Forschern zuzurechnen, wenn ein Zugriff hierauf rechtswidrig sei.[37] In diese Richtung hat auch der Europäische Gerichtshof (EuGH) argumentiert, als er sich mit der Frage der Zurechenbarkeit von Zusatzwissen befasst hat.[38] Danach ist entscheidend, ob der Zugriff auf Zusatzwissen für die verantwortliche Stelle ein Mittel darstelle, dass vernünftigerweise zur Bestimmung der betroffenen Person eingesetzt werden könne.[39] Erst wenn die Verknüpfung gesetzlich verboten oder praktisch undurchführbar und das Risiko einer Identifikation daher faktisch vernachlässigbar sei, dann sei der Zugriff auf das Zusatzwissen durch die verantwortliche Stelle nicht zu erwarten.[40] Nach dem EuGH liege eine praktische Undurchführbarkeit der Verknüpfung dann vor, wenn die Identifikation einen unverhältnismäßig großen Aufwand an Zeit und Kosten erfordern würde.[41] Mithin müsse für die Annahme der Zurechenbarkeit die verantwortliche Stelle über rechtliche Mittel verfügen, um auf das Zusatzwissen zuzugreifen.[42]

Dieser vermittelnde Ansatz mit den Kriterien des EuGH ist überzeugend, da er durch das Abstellen auf rechtliche Mittel in Kombination mit praktischer Umsetzbarkeit den notwendigen Grad an Rechtssicherheit schafft.[43] Die widerstreitenden Interessen des Rechts auf informationelle Selbstbestimmung und der Gewährleistung von Freiheitsgrundrechten wie der Forschungsfreiheit werden in einen verhältnismäßigen Ausgleich gebracht. Den Forschenden wird ein angemessenes Maß an Eigenverantwortung zugeschrieben, ohne etwaige Schutzpflichten in einen Zeitraum vorzuverlegen, in dem kein Gefahrenpotenzial für die betroffene Person besteht.

2. Anonymisierung

Vor diesem Hintergrund und unter Zugrundelegung des EG 26 S. 3 und 4 der DSGVO sowie der einschlägigen Definitionen zur Anonymisierung aus den Landesdatenschutzgesetzen[44] wird von folgender Definition für die Anonymisierung ausgegangen:

> *„Anonymisierung ist das Verändern personenbezogener Daten dergestalt, 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."*[45]

Aus dieser Definition ergeben sich zwei verschiedene Anonymisierungsformen. Einerseits die Form der absoluten Anonymisierung, bei der die Re-Identifikation nicht möglich ist.[46] Andererseits die Form der faktischen Anonymisierung, bei der die Re-Identifikation am unverhältnismäßig hohen Aufwand scheitert.[47] Beide Wege führen dazu, dass die DSGVO aufgrund des entfallenen Personenbezugs der nun vorliegenden Daten nicht anwendbar ist.[48]

Die zugrunde gelegte Definition der Anonymisierung deutet bereits auf eine der zentralen Fragestellungen im Datenschutz hin: Ist eine Anonymisierung tat-

34 Für einen kombinierenden oder vermittelnden Ansatz *Gola*, in Gola/Heckmann (Hrsg.), DS-GVO (2022), 3. Auflage, Art. 4, Rn. 21 ff.; *Spitz/Cornelius*, (Fn. 2), 101 (112 f.); *Brink/Eckhardt*, (Fn. 16), 205 (211); *Buchholtz/Stentzel*, (Fn. 19), Rn. 12.

35 *Buchholtz/Stentzel*, (Fn. 19), Rn. 12.

36 *Spitz/Cornelius*, (Fn. 2), 101 (111).

37 *Buchholtz/Stentzel*, (Fn. 19), Rn. 12.

38 EuGH, 19.10.2016 - C-582/14, MMR (2016), 842 (843 f.), Rn. 45 ff.

39 Ebd., Rn. 45.

40 Ebd., Rn. 46.

41 Ebd., Rn. 46.

42 Vgl. ebd., Rn. 65.

43 *Spitz/Cornelius*, (Fn. 2), 101 (113).

44 Anders als die DSGVO oder das BDSG definieren einige der Landesdatenschutzgesetze die Anonymisierung vgl. mit Abweichungen: § 3 BbgDSG; § 2 Abs. 4 BremDSG; § 11 Abs. 2 HmbDSG. Dabei beziehen diese Normen sich im Grunde auf § 3 Abs. 6 BDSG a.F., der die Anonymisierung legal definierte.

45 Vgl. mit Abweichungen § 3 BbgDSG; § 2 Abs. 4 BremDSG; § 11 Abs. 2 HmbDSG.; im Ergebnis auch EuGH, (Fn. 40), Rn. 46; BfDI, (Fn. 5), 4; vgl. mit Bestätigung der wortgleichen Definition aus § 3 Abs. 6 BDSG a.F. *Gola*, (Fn. 34), Rn. 51.

46 Eine ausschließliche Definition der absoluten Anonymisierung *Ernst*, in: Paal/Pauly (Hrsg.), DS-GVO (2021), 3. Auflage, Art. 4, Rn. 48.

47 Gegen die Möglichkeit der faktischen Anonymisierung *Ernst*, (Fn. 46), Rn. 50; danach führe solch eine „Erschwerung" nur zu einer Pseudonymisierung. Es wird offengelassen, inwiefern dann überhaupt eine Anonymisierung noch tatsächlich möglich ist.

48 Vgl. EG 26 S. 5; *Spindler/Dalby*, in Spindler/Schuster (Hrsg.), Recht der elektronischen Medien (2019), 4. Auflage, Art. 4, Rn. 14.

sächlich umsetzbar? Der BfDI geht in seinem Positionspapier zur Anonymisierung aus dem Jahr 2021 davon aus, dass zumindest eine absolute Anonymisierung nicht möglich sei.[49] Mithin sei also der Schwierigkeitsgrad für eine Re-Identifikation das entscheidende Kriterium für eine (faktische) Anonymisierung. Dieses Kriterium ist kritisch zu bewerten, da die Anforderungen an den „unverhältnismäßig hohen Aufwand" laufend angepasst werden müssen, wenn es KI-Systemen wie Deep Learning (DL) durch Abgleich mit aggregierten Datenbanken möglich ist bzw. sein wird, anonymisierte Daten der betroffenen Person schneller zuzuordnen.[50]

Folglich schließt daran die Notwendigkeit an, dass KI-Systeme gleichzeitig fortschrittlichere Anonymisierungsprozesse ermöglichen, also der Schwierigkeitsgrad der Re-Identifikation proportional dazu wächst.[51] Fraglich ist, ob die state of the art Anonymisierungstechnologien[52] wie k-anonymity[53], l-diversity[54], t-closeness[55] und Differential Privacy[56] diesen dynamischen Fortschritt mitgehen können.

Kritikwürdig an der rechtlichen Definition der Anonymisierung ist zudem, dass sie keine technischen Anforderungen oder bestimmte Anonymisierungstechniken in ihrer Definition enthält, sondern von technischen Standards unabhängig formuliert ist.[57] Folglich stellt die technische Anonymisierung nicht unbedingt eine Anonymisierung im rechtlichen Sinne dar und umgekehrt.[58] Dementsprechend sollte an einer Homogenisierung des technischen und juristischen Anonymisierungsbegriffs gearbeitet werden, um diesbezügliche Diskrepanzen zu beseitigen und Regelungslücken zu vermeiden. Dies würde eine Konkretisierung des rechtlichen Anonymisierungsbegriffs durch technische Aspekte erfordern.[59]

II. Problem der Anonymisierung als Verarbeitung i.S.d. DSGVO

Das zentrale Problem im Zusammenhang mit der Anonymisierung ist die Frage, ob diese sich als eine Datenverarbeitung i. S. d. DSGVO einordnen lässt. Diese Frage wurde auch vom BfDI bisher nicht eindeutig beantwortet. So hat der BfDI zunächst 2017 in seinem Tätigkeitsbericht festgehalten, dass die Anonymisierung keine Datenverarbeitung darstelle.[60] In seinem Positionspapier zur Anonymisierung revidierte er diese Aussage wieder.[61] Die Meinungsänderung ist dogmatisch dünn begründet und erfordert daher eine differenzierte Prüfung des ausschlaggebenden Art. 4 Nr. 2 DSGVO, welcher den Verarbeitungsbegriff legal definiert. Danach bezeichnet der Begriff der Verarbeitung jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Der Art. 4 Nr. 2 DSGVO nennt nachfolgend 18 Regelbeispiele wie die Veränderung, die Verwendung oder das Löschen. Jedoch wird die Anonymisierung nicht ausdrücklich genannt.

Die Anonymisierung wurde auch schon nicht in der Vorgängernorm des Art. 4 Nr. 2 DSGVO dem Art. 2 lit. b

49 So vgl. BfDI, (Fn. 5), 4; auch *Ziebarth*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung (2018), 2. Auflage, Art. 4, Rn. 29 f.

50 Im Ergebnis auch *Ernst*, (Fn. 46), Rn. 50.

51 In diese Richtung ebd.; *Spindler/Dalby*, (Fn. 48), Rn. 16.

52 Eine Übersicht von technischen Anonymitätsverfahren: Leopoldina, Nationale Akademie der Wissenschaften, acatech; Stellungnahme: Privatheit in Zeiten der Digitalisierung (2018), 52 f., abrufbar unter: https://www.leopoldina.org/uploads/tx_leopublication/2018_Stellungnahme_BigData.pdf (zuletzt abgerufen am 08.12.2022).

53 Definition nach Leopoldina, (Fn. 52), 52 f.: k-anonymity soll die Verknüpfung eines sensiblen Attributs zu einem einzelnen Individuum erschweren, da durch Aggregation immer mindestens eine Anzahl von k-Individuen dasselbe sensible Attribut teilt. Ein Set an Daten bietet dann k-Anonymität, wenn die identifizierenden Informationen (Identifier) jedes einzelnen Individuums in dem Datenset von mindestens k-1 anderen Individuen ununterscheidbar sind.

54 Definition nach ebd.: I-diversity garantiert ein Maß an Verschiedenheit der sensiblen Attribute innerhalb einer k-anonymen Gruppe.

55 Definition nach ebd.: t-closeness erweitert das k-anonymity-Modell um einen Parameter, der die Verteilung der sensiblen Attribute in den einzelnen Äquivalenzklassen mit der Verteilung in der gesamten Tabelle harmonisiert.

56 Definition nach ebd.: Differential Privacy erlaubt die Anonymisierung von Datenbeständen sowie anonymisierte Datenbankabfragen. In letzterem Fall behält der Verantwortliche die originalen Daten und erlaubt Dritten statistische Anfragen auf diesen Datenbestand. Die Ergebnisse der Abfragen werden durch hinzugefügte Daten soweit „verrauscht", dass sie in der Menge zwar noch eine korrekte statistische Aussage ermöglichen, das Aussondern (Singling Out) von einzelnen Individuen jedoch verhindern.

57 Ausführlich dazu *Hölzel*, Anonymisierungstechniken und das Datenschutzrecht, DuD (2018), 502 (502).

58 Ebd.

59 Dazu ausführlich *Vokinger/Stekhoven/Krauthammer*, Lost in Anonymization — A Data Anonymization Reference Classification Merging Legal and Technical Considerations, Journal of Law, Medicine & Ethics (2020), 228-231.

60 BfDI, 26. Tätigkeitsbericht zum Datenschutz 2015-2016, 30.05.2017, 170, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/26TB_15_16.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 08.12.2022).

61 BfDI, (Fn. 5), 4.

Datenschutzrichtlinie genannt.[62] Der Art. 2 lit. b Datenschutzrichtlinie wurde nahezu wortgleich übernommen. Im Vergleich dazu hat Art. 4 Nr. 2 DSGVO lediglich noch weitere Beispiele ergänzt. Die Anonymisierung gehörte nicht dazu. Das Fehlen der Anonymisierung legt die erste Annahme nahe, dass die Anonymisierung keine Datenverarbeitung darstellt. Dies gilt es nachfolgend durch weitere Auslegung des Art. 4 Nr. 2 DSGVO zu prüfen.

1. Wortlautauslegung des Art. 4 Nr. 2 DSGVO

Vor dem Hintergrund der Definition der Anonymisierung könnte diese nach dem Wortlaut des Art. 4 Nr. 2 DSGVO eine Veränderung darstellen. Jedoch liegt eine Veränderung nur dann vor, wenn die inhaltliche Umgestaltung der Daten zu einem neuen Informationsgehalt über eine Person führt.[63] Die Anonymisierung soll gerade den Informationsgehalt über eine Person beseitigen und keinen neuen Informationsgehalt hinzufügen.[64] Wenn man diese Änderung der Personenbezogenheit als Veränderung qualifizieren würde, dann könnte die Anonymisierung als Verarbeitung eingeordnet werden.[65] Jedoch würde eine solche Interpretation verkennen, dass der Begriff der Verarbeitung im Zusammenhang mit dem Begriff der personenbezogenen Daten aus Art. 4 Nr. 1 DSGVO gesehen werden muss.[66] Somit ist der Informationsgehalt in Bezug auf die betroffene Person zu ermitteln und von dieser abhängig. Dieser Informationsgehalt des personenbezogenen Datums wird durch die Anonymisierung nicht geändert.[67]

Darüber hinaus kann die Anonymisierung auch nicht mit dem Löschen i. S. v. Art. 4 Nr. 2 DSGVO gleichgestellt werden,[68] da beim Löschen die Daten irreversibel unkenntlich gemacht werden müssen.[69] Zwar ist auch bei der Anonymisierung das Ziel, die Zuordnung der Daten aufzuheben bzw. so zu erschweren, dass eine Re-Identifikation nur mit unverhältnismäßig hohen Mitteln zu erreichen ist. Mithin sind sowohl das Ziel als auch die Wirkungen einer Anonymisierung jedenfalls vergleichbar mit denen einer Löschung.[70] Jedoch führt, wenn überhaupt, nur die absolute Anonymisierung zu einer Art irreversiblen Unkenntlichmachung, wobei auch dann noch das gespeicherte Medium bearbeitbar, auslesbar und wahrnehmbar bleibt.[71] Das Löschen i.S.d. Art. 4 Nr. 2 DSGVO erfordert dahingegen, dass die personenbezogenen Daten nicht mehr verarbeitet, ausgelesen oder wahrgenommen werden können.[72]

Nach Ansicht des BfDI[73] und Teilen der Literatur[74] könnte eine Anonymisierung zumindest eine Verwendung nach Art. 4 Nr. 2 DSGVO sein. Die Verwendung ist ein Auffangtatbestand.[75] Bei einer weiten Auslegung der Verwendung umfasst diese jeden gezielten Umgang mit personenbezogenen Daten.[76] Mithin könnte die Anonymisierung eine Verwendung und damit eine Verarbeitung darstellen, da beim Anonymisierungsprozess personenbezogene Daten gehandhabt werden. Sofern man die Verwendung jedoch als zweckgerichtetes Gebrauchen oder eine interne Nutzung personenbezogener Daten definiert,[77] fällt die Anonymisierung nicht unter Verwendung. Aus dem Grunde, dass die Anonymisierung selbst kein Gebrauchen oder eine Nutzung darstellt. Sie ist vielmehr ein Prozess, der das Gebrauchen und die Nutzung von anonymisierten Daten vorbereiten soll.[78]

Schließlich stellt die Anonymisierung auch kein unbenanntes Beispiel des Art. 4 Nr. 2 DSGVO dar.[79] Dafür bräuchte es eine Begrifflichkeit gleicher Schwere. Es

62 Wortlaut des Art. 2 lit. b Datenschutzrichtlinie: „Verarbeitung personenbezogener Daten“ („Verarbeitung“) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.“

63 *Herbst*, in: Kühling/Wagner, DS-GVO/BDSG (2020), 3. Auflage, Art. 4 Nr. 2 DSGVO, Rn. 25 *Arning/Rothkegel*, (Fn 2), Rn. 78

64 *Arning/Rothkegel*, (Fn 2), Rn. 78; *Thüsing/Rombey*, Anonymisierung an sich ist keine rechtfertigungsbedürftige Datenverarbeitung, ZD (2021), 548 (550); *Gierschmann*, Gestaltungsmöglichkeiten durch systematisches und risikobasiertes Vorgehen, ZD (2021), 482 (484); *Hornung/Wagner*, Anonymisierung als datenschutzrelevante Verarbeitung?, ZD (2020), 223 (224).

65 So BfDI, (Fn. 5), 5; *Gola*, (Rn. 34), Rn. 52; in diese Richtung auch *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (2019), 1. Auflage, Art. 4 Nr. 2, Rn. 20.

66 Vgl. *Arning/Rothkegel*, (Fn 2), Rn. 78; *Thüsing/Rombey*, (Fn. 64), 548 (550).

67 *Arning/Rothkegel*, (Fn 2), Rn. 78.

68 So auch ausführlich *Thüsing/Rombey*, (Fn. 64), 548 (551 f.); *Hornung/Wagner*, (Fn. 64), 223 (224); *Roßnagel*, (Fn. 65), Rn. 30; a.A. *Gola*, (Rn. 34), Rn. 52; *Gierschmann*, (Fn. 64), 482 (484 f.).

69 *Roßnagel*, (Fn. 65), Rn. 30.

70 *Hornung/Wagner*, (Fn. 64), 223 (224).

71 Vgl. *Roßnagel*, (Fn. 65), Rn. 32.

72 Ebd.

73 BfDI, (Fn. 5), 5.

74 *Gola*, (Rn. 34), Rn. 52 f.; BfDI, (Fn. 5), 4; *Hornung/Wagner*, (Fn. 64), ZD (2020), 223 (224).

75 *Roßnagel*, (Fn. 65), Rn. 24; *Ernst*, (Fn. 46), Rn. 29; a.A. *Reimer*, in: Sydow (Hrsg.), Europäische Datenschutzverordnung (2018), 2. Auflage, Art. 4, Rn. 67; mit der Begründung, dass die Verwendung den Modalitäten nach dem Nutzen aus § 3 Abs. 5 BDSG a.F. entspricht, aber es Verarbeitungen gibt, die einen Nutzen, aber keine Verwendung darstellen.

76 So auch *Roßnagel*, (Fn. 65), Rn. 24; BfDI, (Fn. 5), 4.

77 *Ernst*, (Fn. 46), Rn. 29.

78 So auch *Thüsing/Rombey*, (Fn. 64), 548 (550).

79 A.A. BfDI, (Fn. 5), 5; *Roßnagel*, (Fn. 65), Rn. 20.

muss also eine Vergleichbarkeit und Gleichwertigkeit gegeben sein.[80] Der Art. 4 Nr. 2 DSGVO will gerade nicht jeden Umgang mit personenbezogenen Daten erfassen.[81] Das entscheidende Kriterium ist, dass der Umgang mit den personenbezogenen Daten, den darin liegenden Eingriff in das Datenschutzgrundrecht perpetuiert, akzentuiert, verstärkt oder abmildert.[82] Die Beispiele des Art. 4 Nr. 2 DSGVO beschreiben nämlich allesamt Prozesse, die das Datenschutzniveau verändern. Da die Anonymisierung persönlichkeitsneutral ist, betrifft sie eben nicht das Datenschutzniveau.[83] Somit fehlt es an der Vergleichbarkeit und Gleichwertigkeit.

2. Teleologische Auslegung des Art. 4 Nr. 2 DSGVO

Fraglich ist, welche teleologische Argumentation für bzw. gegen eine Qualifikation der Anonymisierung als Verarbeitung spricht. Die Befürworter führen an, dass, wenn bereits das Löschen eine Verarbeitung darstelle, auch die Anonymisierung eine Verarbeitung darstellen müsse.[84] Zudem müsse auch das Interesse der betroffenen Person an einem Erhalt des Personenbezugs geschützt werden.[85] Solch ein Interesse bestehe beispielsweise, um vertragliche Aufbewahrungspflichten Dritten gegenüber zu erfüllen, die personenbezogenen Daten später in einem Rechtsstreit als Beweismittel vorzulegen oder auch nur aus ideellen Gründen weiter verfügbar zu halten.[86] Die entsprechenden Interessen der betroffenen Person am Erhalt ihrer personenbezogenen Daten würden nach Ansicht von *Hornung/Wagner* grundrechtlich durch Art. 8 GRCh und das informationelle Selbstbestimmungsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützt.[87]

Geprägt wird die Ansicht der Befürworter von dem Gedanken, dass der Umgang mit personenbezogenen Daten rechtfertigungsbedürftig sein soll. Die Anonymisierung soll sich nicht im rechtsfreien Raum bewegen.

Jedoch verkennt man hier, dass die Anonymisierung persönlichkeitsneutral ist und gerade Grundrechte und Grundfreiheiten, die durch die DSGVO geschützt werden sollen, grds. nicht tangiert.[88] Wie oben aufgezeigt, ist der Zweck des Art. 4 Nr. 2 DSGVO alle Vorgänge zu erfassen, die das Datenschutzniveau verändern. Eine extensive Auslegung der Norm und Einordnung der Anonymisierung könnte in der Folge vielmehr Freiheitsgrundrechte wie die Forschungs- und Wissenschaftsfreiheit tangieren, da dogmatisch schwer zu begründende Hürden für die Forschenden geschaffen werden würden.

Ferner besteht die Möglichkeit, eine Anonymisierung einer Kopie des in Frage stehenden Datums vorzunehmen.[89] Folglich kann das Löschen und die Anonymisierung nicht einfach gleichstellt werden, da durch den Prozess das ursprüngliche Datum erhalten bleibt. Dies ist beim Löschen gerade nicht der Fall.[90] Mithin verfangen sich dann auch nicht die Bedenken der Befürworter, dass das Interesse der betroffenen Person an dem Erhalt des Personenbezugs des Datums geschützt werden muss. Zumal aus dem Datenschutzgrundrecht nach Art. 8 GrCH auch kein Recht auf Speicherung, auf dem ein solches Interesse basiert werden könnte, fließt.[91] Die Speicherung ist danach eine Verarbeitungsform, in die die betroffene Person einwilligen kann, aber auf die kein Anspruch der betroffenen Person besteht.[92]

3. Systematische Probleme

Schließlich würde die Einordnung der Anonymisierung als Verarbeitung auch systematische Probleme kreieren, die überzeugend gelöst werden müssten. Wenn nämlich die Anonymisierung eine Verarbeitung ist, dann fällt diese Verarbeitung unter das Verbotsprinzip der DSGVO. Mithin braucht es eine Rechtsgrundlage für die Anonymisierung von personenbezogenen Daten.

Als Rechtsgrundlage kommt zunächst die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO in Betracht. Aber auch ohne Einwilligung könnte eine Anonymisierung aufgrund der Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO oder aufgrund von überwiegenden berechtigten Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO erfolgen.[93] Bei letzterer Möglichkeit werden die gegenseitigen Interessen der Be-

80 *Thüsing/Rombey*, (Fn. 64), 548 (550).
81 Ebd.; in diese Richtung auch *Gola*, (Rn. 34), Rn. 53 f.; a.A. *Roßnagel*, (Fn. 65), Rn. 10; *Hornung/Wagner*, (Fn. 64), 223 (224).
82 *Thüsing/Rombey*, (Fn. 64), 548 (550).
83 Ebd.
84 Vgl. *Hornung/Wagner*, (Fn. 64), 223 (224 f.); vgl. *Gierschmann*, (Fn. 64), 482 (485).
85 *Hornung/Wagner*, (Fn. 64), 223 (225).
86 Ebd.
87 Ebd.
88 *Thüsing/Rombey*, (Fn. 64), 548 (550); im Grunde auch *Hornung/Wagner*, (Fn. 64), 223 (225), die ebenfalls die Anonymisierung als Schutzinstrument qualifizieren.
89 *Thüsing/Rombey*, (Fn. 64), 548 (552).
90 Vgl. ebd.
91 Ebd.; vgl. *Jarass*, in: Jarass, GrCh (2021), 4. Auflage, Art. 8 GrCh, Rn. 9 f.
92 Vgl. ebd., vgl. *Thüsing/Rombey*, (Fn. 64), 548 (552).
93 Ausführlich zu den in Frage kommenden Rechtsgrundlagen *Hornung/Wagner*, (Fn. 64), 223 (225 ff.); darauf verweisend *Gierschmann*, (Fn. 64), 482 (485).

teiligten gegeneinander abgewogen. Die Anonymisierung hat dann zu unterbleiben, wenn die Interessen oder die Grundrechte und Grundfreiheiten, die den Schutz der personenbezogenen Daten erfordern, überwiegen.[94]

Fraglich ist jedoch, welche Anforderungen an die Anonymisierung von Gesundheitsdaten bestehen. Dafür muss man sich zunächst die Struktur von Art. 9 DSGVO vergegenwärtigen. Der erste Absatz verbietet die Verarbeitung besonderer Kategorien von Daten. Das sind besonders sensible, also schutzwürdige Daten wie beispielsweise Gesundheitsdaten oder genetische Daten. Der zweite Absatz wiederum normiert Ausnahmetatbestände wie die Einwilligung, nach denen eine Verarbeitung und eine Anonymisierung potenziell durchgeführt werden könnten. Der Kreis der Tatbestände, nach denen eine Anonymisierung stattfinden kann, ist ohne die Einwilligung begrenzt. In Betracht kommt das sog. Forschungsprivileg nach Art. 9 Abs. 2 lit. j DSGVO bzw. § 27 BDSG. Daneben ist für viele Tatbestände des Art. 9 Abs. 2 DSGVO die Ausgestaltung nicht abschließend geklärt, da für einige der Ausnahmen noch konkrete unionsrechtliche oder mitgliedsstaatliche Regelungen erforderlich sind.[95] Somit erscheint es fraglich, ob diese Ausnahmetatbestände, die grds. restriktiv auszulegen sind, eingreifen.[96] Zudem sieht der Art. 9 Abs. 2 DSGVO auch keine Möglichkeit vor, die dem Art. 6 Abs. 1 S. 1 lit. e DSGVO entspricht, der eine Anonymisierung bei überwiegendem Interesse zulassen würde. Das bedeutet, dass selbst wenn eine Anonymisierung im Interesse aller Beteiligten ist, diese nicht durchgeführt werden kann.[97]

Insgesamt führt die Qualifikation der Anonymisierung als Verarbeitung dazu, dass ein Wertungswiderspruch offenbart wird.[98] Die Anonymisierung besonderer Kategorien personenbezogener Daten wäre bei einem solchen Verständnis unter strengeren Voraussetzungen möglich als die Anonymisierung einfacher personenbezogener Daten. Mithin wird der betroffenen Person ein Schutzinstrument vorenthalten. Dabei sollte es vor dem Hintergrund des Datenschutzgrundrechts genau andersherum sein. Die Anonymisierung, die dem Schutz der betroffenen Person dient, müsste für im besonderen Maße schützenswerte Daten i.S.d. Art. 9 DSGVO leichter möglich sein.[99] An die Anonymisierung sensibler Daten strengere Anforderungen stellen zu wollen als an die Anonymisierung von einfachen Daten, ist daher unbestritten systemwidrig.[100]

4. Lösungsansatz der teleologischen Reduktion des Art. 4 Nr. 2 DSGVO

Dieses systematische Problem wollen *Hornung/Wagner* mit einer teleologischen Reduktion des Art. 9 Abs. 1 DSGVO lösen.[101] Die Voraussetzung für eine teleologische Reduktion ist, dass die vom Wortlaut erfassten Fälle der Zielsetzung des Gesetzes widersprechen.[102] So wird von *Hornung/Wagner* argumentiert, dass es die Zielsetzung des Gesetzgebers mit Art. 9 Abs. 1 DSGVO ist, einen zusätzlichen Schutz zu schaffen, da die Verarbeitung von sensiblen Daten ein erhöhtes Risiko für Grundrechte und –freiheiten darstelle.[103] Die Anonymisierung sei jedoch grundsätzlich persönlichkeitsneutral und steigere das Eingriffsniveau in Grundrechte und Grundfreiheiten grundsätzlich nicht. Somit würden die hohen Hürden für die Anonymisierung das Risiko für die Rechte der betroffenen Person mangels des Schutzinstruments der Anonymisierung erhöhen. Dies würde einen Widerspruch zur Zielsetzung des Gesetzgebers darstellen.[104] Folglich müsse eine teleologische Reduktion des Verbots in Art. 9 Abs. 1 DSGVO stattfinden. Dadurch würde für eine Anonymisierung sensibler Daten Art. 6 Abs. 1 S. 1 lit. e DSGVO beispielsweise zur Anwendung gelangen.[105] Die schutzwürdigen Interessen der betroffenen Person würden in die Abwägung einfließen und wären damit gewahrt.

Gegen eine teleologische Reduktion spricht, dass der hohe Schutzstandard von Art. 9 Abs. 1 DSGVO nicht leichtfertig teleologisch reduziert werden sollte. Zumal dies auch das Tor zu weiteren teleologischen Reduktionen öffnen könnte.[106] Darüber hinaus existiert bisher keine Praxis des EuGH zur teleologischen Reduktion des Sekundärrechts.[107] Vielmehr legt der EuGH das Sekundärrecht extensiv aus und hält die Mitgliedstaaten eher

94 *Hornung/Wagner*, (Fn. 64), 223 (225).
95 Überblick dazu *Mester*, in: Taeger/Gabel (Hrsg.), DSGVO – BDSG (2022), 4. Auflage, Art. 9 DSGVO, Rn. 17 ff.
96 So auch *Hornung/Wagner*, (Fn. 64), 223 (226).
97 Ebd.
98 So auch *Thüsing/Rombey*, (Fn. 64), 548 (552); *Gierschmann*, (Fn. 64), 482 (485); *Hornung/Wagner*, (Fn. 64), 223 (226); die Problematik andeutend und verweisend *Gola*, (Rn. 34), Rn. 52.
99 *Thüsing/Rombey*, (Fn. 64), 548 (552); vgl. *Hornung/Wagner*, (Fn. 64), 223 (226).
100 *Thüsing/Rombey*, (Fn. 64), 548 (552); vgl. *Gierschmann*, (Fn. 64), 482 (485); im Ergebnis vgl. *Hornung/Wagner*, (Fn. 64), 223 (226).
101 *Hornung/Wagner*, (Fn. 64), 223 (227); ebenso *Stürmer*, Löschen durch Anonymisieren?, ZD (2020), 626 (631); einen anderen Vorschlag macht *Gierschmann*, der die Anonymisierung als Löschen qualifiziert, wonach der Wertungswiderspruch vermieden werde; siehe dazu *Gierschmann*, (Fn. 64), 482 (485).
102 *Hornung/Wagner*, (Fn. 64), 223 (227).
103 Ebd.
104 Ebd.
105 Ebd.
106 *Thüsing/Rombey*, (Fn. 64), 548 (552 f.).
107 Ebd.

dazu an, nationales Recht entsprechend zu reduzieren.[108]

5. Zwischenfazit

Dogmatisch lässt sich eine Einordnung der Anonymisierung als Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO schwerlich begründen. Weder der Wortlaut noch eine etwaige teleologische Auslegung liefern überzeugende Argumente. Vielmehr würde die Qualifikation der Anonymisierung zu systematischen Widersprüchen führen, wonach die Anonymisierung von sensiblen Daten i. S. d. Art. 9 DSGVO nur unter höheren rechtlichen Hürden durchführbar wäre als die Anonymisierung von einfachen personenbezogenen Daten. Der hierbei vorgebrachte Ansatz der teleologischen Reduktion des Art. 9 DSGVO vermag angesichts des besonderen Schutzgutes und der fehlenden Rechtsübung des EuGH hinsichtlich der teleologischen Reduktion des Sekundärrechts den Wertungswiderspruch nicht zu lösen.

III. Anonymisierung als Chance für die Sekundärforschung

Vor diesem Hintergrund scheint die Anonymisierung als Verfahren, das neben der DSGVO besteht, eine Chance für die Forschung und Wissenschaft, insbesondere hinsichtlich der Sekundärnutzung von besonderen Kategorien von Daten i. S. d. Art. 9 DSGVO, zu sein. Sie stellt eine Alternative zum Forschungsprivileg nach Art. 9 Abs. 2 lit. j DSGVO dar. Diese zentrale Norm eröffnet Forschenden die Möglichkeit, Daten auch ohne Einwilligung der betroffenen Personen zu erheben. Danach ist eine Abwägung der Interessen der Forschenden und der betroffenen Person vorzunehmen. Die Verarbeitung ist dabei legitim, soweit die Verarbeitung für die Forschungszwecke erforderlich ist, das Forschungsziel im angemessenen Verhältnis zum Datenschutz der betroffenen Person steht und geeignete Garantien nach Art. 89 Abs. 1 DSGVO getroffen werden. Bei einer Anonymisierung würde man diese notwendige Interessenabwägung und weitere Hürden im Zusammenhang mit dem Forschungsprivileg vermeiden.[109]

Dass eine Anonymisierung von besonderen Kategorien von Daten auch möglich sein soll, zeigt sich in § 27 Abs. 3 S. 1 BDSG, der eine frühestmögliche Anonymisierung im Rahmen der Datennutzung und -verarbeitung für die Forschung und Wissenschaft vorschreibt. Dabei ist für die Forschenden besonders wichtig, dass die DSGVO die faktische Anonymität ausreichen lässt, da eine absolute Anonymisierung unter Umständen, wie oben dargestellt, einer Löschung entsprechen würde. Die Löschung des Personenbezugs kann regelmäßig den Forschungsinteressen entgegen stehen, da z. B. Langzeitstudien eine fortlaufende Zuordnung neuer Daten zu bereits vorhandenen Daten erfordern.[110] Bei Langzeitstudien steht die Wirksamkeit von Therapien und Umweltfaktoren oft erst nach Jahren fest.[111]

Die faktische Anonymisierung ist besonders bei genetischen Daten oder Biomaterialien der einzig mögliche Weg, da hier wegen der darin enthaltenen Erbinformation ein inhärenter Personenbezug besteht.[112] Dieser Umstand führt dazu, dass eine absolute Anonymisierung unmöglich ist.[113] Obwohl genetische Daten sich unverwechselbar auf eine natürliche Person beziehen, benötigt die verantwortliche Stelle weiteres Referenzwissen, um die hinter dem Datum stehende natürliche Person eindeutig zu identifizieren oder ausreichend einzugrenzen.[114] Sofern ein solches Referenzwissen zur Verfügung steht, eröffnet dies die Möglichkeit mittels eines sog. Matching-Verfahrens die genetischen Daten einer bestimmten Person zuzuordnen.[115] Angesichts der dynamischen Entwicklung von Erzeugung, Erfassung sowie Auswertung medizinischer Forschungsdaten und Zunahme von frei zugänglichem Referenzwissen sind die faktischen Möglichkeiten einer Anonymisierung von genetischen Daten oder Gesundheitsdaten zunehmend begrenzt.[116]

IV. Bewertung des Schutzbedarfs für anonymisierte Daten

Auch wenn sich der Prozess der Anonymisierung, wie dargestellt, dogmatisch schwer unter den Anwendungsbereich der DSGVO fassen lässt, bedeutet das nicht, dass

108 *Thüsing/Rombey*, (Fn. 64), 548 (552 f.); ein Beispiel dafür EuGH, 10.12.2020 – C-735/19, WM (2021), 16, Rn. 76.

109 Ausführlich zum Forschungsprivileg *Becker*, (Fn. 31), 103-114.

110 *Krawczak/Weichert*, Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland (2017), 7, abrufbar unter: https://www.uni-kiel.de/medinfo/documents/TWMK%20Vorschlag%20DInfMedForsch%20v1.9%20170927.pdf (zuletzt abgerufen am 08.12.2022).

111 Ebd.

112 Ebd.; *Spitz/Cornelius*, (Fn. 2), 101 (104).

113 *Krawczak/Weichert*, (Fn. 110), 7.

114 *Spitz/Cornelius*, (Fn. 2), 101 (105); *Arning/Forgó/Krügel*, Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DuD (2006), 700 (701).

115 *Spitz/Cornelius*, (Fn. 2), 101 (105); *Arning/Forgó/Krügel*, (Fn. 116), 700 (701).

116 *Spitz/Cornelius*, (Fn. 2), 101 (105).

die im Anschluss an die Anonymisierung erhaltenen anonymisierten Daten keinen weiteren Schutz bedürfen. Zum einen hängt in der Praxis die Wahrscheinlichkeit einer Re-Identifikation stark davon ab, wer Zugang zu den Daten hat und welche Methoden und Hilfsmittel hierfür eingesetzt werden.[117] So ändern sich die anzuwendenden Kriterien Kosten, Zeitaufwand und Technologie mit der Zeit durch den Fortschritt im Bereich von Data Science, Big Data und Künstlicher Intelligenz.[118] Folglich wächst auch die Wahrscheinlichkeit, dass eine solche Re-Identifikation technisch schneller möglich wird. Es ist klärungsbedürftig, wie man dem Risiko der Re-Identifikation nachhaltig entgegentritt. Dieses spezielle Risiko offenbart das größte Problem bei der Bewertung der Anonymisierung und von anonymisierten Daten: Die binäre Unterteilung in anonyme bzw. anonymisierte Daten einerseits und personenbezogene Daten andererseits. Sie spiegelt die tatsächlichen Verhältnisse und technischen Möglichkeiten nicht wider. Diese Unterteilung ist zu einfach.[119] Die rechtsdogmatische Komplexität der Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten zeigte sich bereits in der oben dargestellten Diskussion zur Identifizierbarkeit von Daten.

Vor dem Hintergrund des oben zur Zurechenbarkeit von Zusatzwissen von Dritten im Rahmen der Bewertung der Identifizierbarkeit von Daten Besprochenen ist die Anonymität von Daten abhängig von zwei entscheidenden Faktoren: Dem Datum und dem Datenbesitzer. Daraus folgt die Überlegung, dass es eine Einschränkung des Datenbesitzers von anonymisierten Daten geben muss, da die Daten bei einem Besitzer anonymisiert, jedoch beim anderen personenbezogen sein können.[120] Der Gedanke, dass es Vorschriften darüber geben muss, welche Daten, in welcher Form, bei welchem Nutzer sein dürfen, spiegelt sich auch in den oben genannten Kriterien des EuGH zur Zurechnung von Zusatzwissen wider.[121] Danach erfolgt eine Zurechnung des Zusatzwissens für die verantwortliche Stelle nicht, wenn ihr der Zugriff auf das Wissen rechtlich oder tatsächlich nicht möglich nicht. Diese Kriterien könnten eine Grundlage für die Regulierung des Umgangs mit anonymisierten Daten bilden. Jedoch zeigt die oben dargestellte Diskussion, dass es keine Einigkeit hinsichtlich der Bewertung der Zurechenbarkeit gibt. Daneben ist auch die Umsetzbarkeit der EuGH-Kriterien fraglich, da eine laufende Neubewertung der tatsächlichen Gegebenheiten erforderlich sein müsste. Hinzu kommt, dass es keinerlei Beschränkungen gegen die Weitergabe der anonymisierten Daten an Dritte mehr gibt, da diese Daten nicht dem Schutzregime der DSGVO unterliegen. Auch eine Veröffentlichung von anonymisierten Daten birgt die Gefahr, dass diese Daten bei Dritten landen, die über die technischen Möglichkeiten verfügen, durch Datenaggregation eine Re-Identifikation herbeizuführen.[122]

Ein weiterer Aspekt ist, dass durch die Anonymisierung Probleme auch erst entstehen können. So entfallen die Betroffenenrechte nach Art. 12 bis 23 DSGVO durch die Anonymisierung, da anschließend die Zuordnung zwischen Daten und der betroffenen Person nicht mehr möglich ist. Beide Punkte zusammengenommen bilden die Basis für die Forderung von *Kneuper*, dass auch für anonymisierte Daten aus Datenschutzsicht ein Schutz erforderlich ist.[123] Danach sollte die Anonymisierung als eine Maßnahme (von mehreren möglichen) zum Datenschutz verstanden werden. Diese Maßnahme trägt in vielen Fällen wesentlich zum Schutz der Daten und damit der betroffenen Person bei, gewährleistet aber keinen vollständigen Schutz der betroffenen Person.[124]

1. Problemlösung

Es existieren verschiedene Ansätze, wie mit den Herausforderungen und Risiken, welche durch die Anonymisierung bzw. für die anonymen oder anonymisierten Daten bestehen, umgegangen werden kann. Im Folgenden werden einige dieser Ansätze vorgestellt.[125]

a) Einführung einer Beobachtungspflicht

Ein Lösungsansatz ist die Einführung einer Beobachtungspflicht. Danach wird der Verantwortliche verpflichtet, die Entwicklung in Bezug auf neue Verfahren oder andere Daten, mit deren Hilfe eine Re-Identifikation möglich wäre, zu beobachten und bei Bedarf die bereitgestellten anonymen Daten zurückzuziehen.[126] Angesichts dessen, dass eine Veröffentlichung von anonymisierten oder personenbezogenen Daten nicht rückgängig gemacht werden kann, ist die Effektivität des Lösungsansatzes fraglich. Letztlich stellt eine Beobach-

117 Siehe Ausführungen unter I.
118 Im Ergebnis auch *Ernst*, (Fn. 46), Rn. 50.
119 So auch *Kneuper*, Anonymisierte Daten brauchen keinen Datenschutz – wirklich nicht?, in: Friedewald et al. (Hrsg.), Selbstbestimmung, Privatheit und Datenschutz (2022), 171 (176).
120 Ebd., 173.
121 EuGH, (Fn. 38), Rn. 45.
122 *Kneuper*, (Fn. 119), 171 (173).
123 Ebd., 175.
124 Ebd., 176.
125 Ausführlich dazu ebd., 171-188; *Ohm*, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Rev. 57 (2010), 1701-1777.
126 *Kneuper*, (Fn. 119), 171 (181).

tungspflicht nur eine Lösung für die spezielle Situation dar, in der immer wieder neue, aktualisierte Fassungen der anonymisierten Daten veröffentlicht werden, was dann bei Bedarf gestoppt werden kann.[127] Darüber hinaus sind Einzelfälle denkbar, in denen die Daten nur für begrenzte Zeit Schutz erfordern, so dass die Veröffentlichung zwar nicht rückgängig gemacht werden kann, später aber keinen Schaden mehr verursacht.[128] Mithin ist eine Beobachtungspflicht als alleinige Lösung unzulänglich. Zumal sie den Verantwortlichen eine Pflicht aufbürden würde, die unter Umständen einen hohen zeitlichen und technischen Aufwand erfordert. Fraglich ist dann, ob bei Zugrundelegung von Kosten-Nutzen-Erwägungen eine Beobachtungspflicht nicht eine Hürde darstellt, die den Verantwortlichen in dem Maße belastet, dass er von einer Anonymisierung oder einer Veröffentlichung von anonymisierten Daten absieht. Dieser Umstand könnte wiederum einen negativen Effekt für Forschungsvorhaben haben, die auf den Zugang von Open Data angewiesen sind. Damit könnte die Einführung einer Beobachtungspflicht die Forschungsfreiheit beschränken, obwohl sie den Datenschutz voraussichtlich nur sehr begrenzt fördert.

b) Verbot der Re-Identifikation

Ein weiterer Ansatz wäre es, die Re-Identifikation von anonymisierten Daten grundsätzlich zu verbieten.[129] Die Re-Identifikation ist zwar implizit auch durch die DSGVO verboten, weil es keine Rechtsgrundlage für diese Verarbeitung personenbezogener Daten gibt.[130] Jedoch wird argumentiert, dass ein explizites Verbot der Re-Identifikation zur Lösung des Problems der Gefahr der Re-Identifikation beitragen könne.[131] Zusätzlich müsse auch die Weitergabe und Weiterverarbeitung von anonymisierten Daten beschränkt werden und eine Löschpflicht für nicht mehr notwendige anonyme Daten eingeführt werden.[132] Dennoch wird das Verbot der Re-Identifikation das Problem nicht vollständig lösen können, da einerseits ein gesetzliches Verbot allein nicht verhindern wird, dass Besitzer der Daten außerhalb des Geltungsbereiches des jeweiligen Gesetzes die Daten re-identifizieren.[133] Andererseits ist es auch innerhalb des Geltungsbereiches schwierig zu erkennen, wann ein Besitzer eine Entscheidung auf Grund einer verbotenen Re-Identifikation getroffen hat bzw. wann überhaupt eine Re-Identifikation erfolgt ist.[134] Hier zeigt sich auch ein Grundproblem bei der Einführung von Verboten und Pflichten, nämlich die Gefahr von Umsetzungsdefiziten. Es ist fraglich, wie und durch wen die Kontrolle der Umsetzung eines Re-Identifikationsverbotes gewährleistet werden kann. Der Einblick in die Datenverarbeitungsabläufe bei Verantwortlichen, die über große Datensätze und fortschrittlichste Verarbeitungstechniken verfügen, ist aufgrund von ggfs. mangelnder Expertise und hohem zeitlichen Mehraufwand beschränkt.[135] *Roßnagel/Geminn* schlagen vor, die Durchsetzung eines Re-Identifikationsverbots durch eine Abschreckung durch hohe Bußgelder zu gewährleisten.[136]

Schließlich ist *Kneuper* dahingehend zuzustimmen, dass es eine Herausforderung wäre, in einem solchen Gesetz zwischen legitimen Gründen für eine Re-Identifikation und den zu verbietenden nicht legitimen Gründen zu unterscheiden.[137] Für einige Forschungswecke ist es bspw. notwendig, dass zumindest eine Möglichkeit der Re-Identifikation besteht. Mithin bedarf es eines ausdifferenzierten Verbotes. Sofern man die Gefahr des Umsetzungsdefizites ausklammert, besteht das Potential, dass ein solches gesetzliches Verbot der Re-Identifikation als Ergänzung weiterer Maßnahmen helfen, aber die beschriebenen Probleme nicht allein lösen können wird.[138]

c) Ausformulierung konkreter Anforderungen an den Grad der Anonymisierung

Schließlich existieren Lösungsansätze, die ein Bewertungssystem vorsehen, wonach der Grad der Anonymität von Daten bzw. der Grad der Anonymisierung durch entsprechende Anonymitätsmodelle bestimmt wird. Mithin würde dies einen Anonymisierungsbegriff erfordern, der die rechtlichen und technischen Aspekte miteinander verbindet. Im Zusammenhang mit diesem Lösungsansatz werden die bereits oben erwähnten Ano-

127 *Kneuper*, (Fn. 119), 171 (181).
128 Ebd.
129 So beispielsweise in Großbritannien in Sect. 171 UK Data Protection Act (2018), abrufbar unter https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (zuletzt abgerufen am 08.12.2022); auch *Roßnagel/Geminn*, Vertrauen in Anonymisierung, ZD (2021), 487 (488).
130 *Kneuper*, (Fn. 119), 171 (183).
131 Vgl. *Roßnagel/Geminn*, (Fn. 129), 487 (488).
132 Ebd.
133 *Kneuper*, (Fn. 119), 171 (183).
134 Ebd.; *Ohm*, (Fn. 125), 1701 (1758).
135 Dazu auch *Ohm*, (Fn. 125), 1701 (1758).
136 *Roßnagel/Geminn*, (Fn. 129), 487 (490); danach wäre zudem die Einführung eines Straftatbestandes der willentlichen Re-Identifikation sinnvoll.
137 *Kneuper*, (Fn. 119), 171 (183).
138 Ebd., 188.

nymitätsmodelle wie die k-anonymity, l-diversity und Differential Privacy genannt.[139] Die Bewertungsverfahren könnten konkret dazu genutzt werden, um ein Mindestmaß an erreichter Anonymität zu fordern. Der Grad der Anonymität wäre von dem mit einer Re-Identifikation verbundenen Risiko für die betroffene Person abhängig.[140] Ein Beispiel für eine entsprechende erforderliche Regel liefert *Kneuper*, wie folgt:

> *„Um anonymisierte Daten zu veröffentlichen, die höchstens ein mittleres Risiko darstellen und deren Urbild keine personenbezogenen Daten besonderer Kategorien enthält, muss mindestens eine l -Diversität mit einem Wert l = . . . nachgewiesen werden".*[141]

Mithin ist *Kneuper* dahingehend zuzustimmen, dass dieser Lösungsansatz eine Bereitstellung von anonymisierten Daten für Forschungszwecke erlauben würde, gleichzeitig aber auch ein gewisses Mindestmaß an Anonymität sicherstellen würde.[142]

Dieser Lösungsansatz ist an die US-amerikanischen HIPAA-Regelungen für die Anonymisierung von Gesundheitsdaten angelehnt, welche aus zwei Varianten bestehen.[143] Nach der ersten Variante ist eine Expertenbewertung („expert determination"-method) der Anonymisierung, typischerweise basierend auf Anonymitätsmodellen, ohne dabei aber konkrete Modelle oder Parameter vorzugeben, durchzuführen.[144] Dahingegen definiert die zweite Variante („safe harbor"-method) konkrete Attribute, die bei der Anonymisierung von Gesundheitsdaten entfernt bzw. zumindest generalisiert werden müssen.[145]

d) Zwischenfazit

Die verschiedenen Lösungsansätze wie die Beobachtungspflicht und das Verbot der Re-Identifikation schaffen es nur Teilaspekte der mit der Anonymisierung und für anonymisierte Daten verbundenen Risiken zu bewältigen. Sie sind nicht vollends überzeugend, können aber als Ergänzungsmaßnahmen in Betracht gezogen werden, wobei bei diesen beiden Lösungsansätzen ein erhöhtes Risiko eines Umsetzungsdefizites besteht. Überzeugender ist vielmehr die Ausformulierung von konkreten Anforderungen an den Grad der Anonymisierung. Genau diese Homogenisierung zwischen technischen und rechtlichen Aspekten der Anonymisierung ist erforderlich, um auf die schnelllebigen technisch-organisatorischen Entwicklungen zu reagieren. Hierbei überzeugt die Variante 2 der US-amerikanischen HIPAA-Regelungen. Denn anders als *Kneuper* argumentiert, gewährleistet ein ausformuliertes Verfahren mit konkreten Parametern, nicht nur die Transparenz des Verfahrens, sondern die Umsetzbarkeit wird auch für Laien vereinfacht. Eine erfolgsorientierte Lösung, wie die Variante 1 es vorsieht und für die *Kneuper* plädiert, ist nur durch eine Expertenbewertung zuverlässig zu gewährleisten. Dies eröffnet wiederum ein erhöhtes Risiko des Umsetzungsdefizites, denn eine Expertenbewertung setzt Experten voraus. Zunächst müsste geklärt werden, welche Kriterien einen Experten ausmachen, wie viele Experten für die Bewertung notwendig sind und ob die Experten externe Personen sein müssen. Der Prozess der Anonymisierung wird durch weitere Hürde möglicherweise zeit- und kostenintensiv verlängert. Zudem setzt die Expertenbewertung kein Modell oder Parameter voraus, dies wiederum kann die Nachvollziehbarkeit von Entscheidungen beeinflussen. Zumal auch die Chancengleichheit unter Umständen tangiert werden kann, denn einheitliche Modelle und Parameter haben den Vorteil, dass sie eine einheitliche Bewertungsgrundlage darstellen. Die Gefahr, dass die Experten gleiche Sachverhalte anders bewerten, reduziert sich. Nichtsdestotrotz kann der Einsatz einer Expertenbewertung basierend auf einem konkret definierten Anonymitätsmodell mit konkreten Parametern für die Anonymisierung insbesondere bei der Bewertung der Anonymisierung besonderer Kategorien von Daten wie Gesundheitsdaten oder genetische Daten erforderlich sein. Damit kann verhältnismäßig auf die Steigerung der Schutzbedürftigkeit der Daten reagiert werden und eine Sicherheitsvorkehrung mehr geschaffen werden.

Abschließend ist festzuhalten, dass die verschiedenen Lösungsansätze die angesprochene Problematik hinsichtlich des Schutzbedürfnisses von anonymisierten Daten nicht vollständig klären können.[146] Dies bedeutet jedoch nicht, dass die Anonymisierung keine geeignete

139 Siehe Ausführungen unter I. 2.
140 *Kneuper*, (Fn. 119), 171 (182).
141 Ebd.
142 Ebd.
143 Office for Civil Rights (OCR): Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule (2012), abrufbar unter https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (zuletzt abgerufen am 08.12.2022).
144 Ebd., 7.
145 Ebd., 7 f.
146 So auch im Ergebnis *Kneuper*, (Fn. 119), 171 (182).

Datenschutzmaßnahme darstellt und nicht mehr durchgeführt werden sollte.[147] Insbesondere der hier aufgezeigte Ansatz der Konkretisierung von Anonymisierungsanforderungen im Zusammenhang mit technischen Anonymisierungsmodellen gepaart mit der für sensible Daten erforderlichen Expertenbewertung könnte Datenschutzbedenken zumindest entgegenwirken.

V. Pseudonymisierung als Alternative

Allerdings lassen sich die datenschutzrechtlichen Risiken beim Umgang mit genetischen Daten oder Gesundheitsdaten alternativ auch durch den Einsatz von Pseudonymen und die isolierte und kontrollierte Verarbeitung der Daten maßgeblich verringern. Die Pseudonymisierung kann unter Umständen auch die verschiedenen Forschungsinteressen, die bei der Nutzung von genetischen Daten und Gesundheitsdaten für Forschungszwecke bestehen, in Einklang bringen. Zum einen existiert das Interesse am überindividuellen Erkenntnisgewinn, welches losgelöst von dem hinter dem Datum stehenden individuellen Patienten besteht.[148] Dafür bräuchte es keine Re-Identifikationsmöglichkeit des konkreten Patienten. Zum anderen ist jedoch bereits im Behandlungskontext aufgrund der Dokumentationspflicht nach § 630 lit. f BGB der Erhalt der Identifikationsmöglichkeit erforderlich.[149] Darüber hinaus kann die Re-Identifikationsmöglichkeit der Daten auch für die Forschungsnutzung von Interesse sein. Eine fortwährende Zuordnungsmöglichkeit würde eine Vorsorgemaßnahme darstellen, um bspw. Redundanzen innerhalb verschiedener Datensätze aus unterschiedlichen Quellen und unterschiedlichen Zeiträumen durch korrekte Zuordnung vorzubeugen.[150]

Nach der Legaldefinition des Art. 4 Nr. 5 DSGVO ist Pseudonymisierung das Ersetzen von Identifikationsmerkmalen durch ein Kennzeichen und die getrennte Aufbewahrung dieser zusätzlichen Informationen, um die Identifikation der betroffenen Person auszuschließen. Dabei werden die identifizierenden Elemente des Datums nicht gelöscht, sondern durch einen Zuordnungsschlüssel ersetzt, der die Wiederherstellung des Personenbezugs ermöglicht.[151] Dieser Prozess führt zu getrennten Datensätzen[152], die auch eine getrennte rechtliche Bewertung zur Folge haben.[153]

Vor dem Hintergrund des oben besprochenen EG 26 Satz 2 DSGVO handelt es sich bei pseudonymisierten Daten, die durch Heranziehen zusätzlicher Informationen einer natürlichen Person zugeordnet werden können, um personenbezogene Daten.[154] Somit ist das Datum auch nach der Pseudonymisierung ein personenbezogenes Datum für die Stelle, die sowohl über die Identifikationsmerkmale als auch den Zuordnungsschlüssel verfügt. Dahingegen wirkt im Bereich der Fremdforschung die Pseudonymisierung aus Sicht der Stelle, die ausschließlich Daten ohne Zuordnungsschlüssel und Identifikationsmittel besitzt, als Anonymisierung. Zu diesem Ergebnis führt die Anwendung des vorzugswürdigen vermittelnden Ansatzes, wonach die Identifizierbarkeit von der konkret zu betrachtenden Stelle und das ihr rechtlich und praktisch zur Verfügung stehende Wissen abhängt.[155]

Folglich ist festzuhalten, dass die Pseudonymisierung durchaus eine Maßnahme darstellt, die zum einen die verschiedenen Forschungsinteressen hinsichtlich der Nutzung von genetischen Daten und Gesundheitsdaten in einen angemessenen Ausgleich bringen kann. Zum anderen ist die Pseudonymisierung nach Art. 25 Abs. 1 DSGVO ein Beispiel datenschutzfreundlicher Voreinstellung und nach Art. 32 Abs. 1 lit. a DSGVO ist die Pseudonymisierung ein Element technischer und organisatorischer Maßnahmen.[156] Die Pseudonymisierung führt anders als die Anonymisierung letztlich auch dazu, dass die Schutzvorschriften der DSGVO genau für die Stellen weiterhin gelten, die über den größten Zugang zu sensiblen Informationen verfügen. In der Folge werden über den vermittelnden Ansatz und dessen Bedeutung für die fak-

147 A.A. ausführlich bei *Zibuschka et al.,* Anonymization is dead – long live privacy. in: Roßnagel/Wagner/Hühnlein (Hrsg.), Open Identity Summit (2019), 71–82.

148 *Spitz/Cornelius*, (Fn. 2), 101 (105); vgl. *Krawczak/Weichert*, (Fn. 110), 7.

149 *Spitz/Cornelius*, (Fn. 2), 101 (105); BT-Drs. 17/10488, 25 f., abrufbar unter https://dserver.bundestag.de/btd/17/104/1710488.pdf (zuletzt abgerufen am 08.12.2022).

150 *Spitz/Cornelius*, (Fn. 2), 101 (106 f.).

151 *Arning/Rothkegel*, (Fn. 2), Rn. 125.

152 Anschließend kann für die Aufgabe der Erstellung und Verwahrung der getrennten Datensätze an eine Datentreuhandstelle übertragen werden. Die Datentreuhandstelle verwaltet das Pseudonym und ist organisatorisch zwischen die datenhaltende und die forschende Stelle geschaltet; dazu *Spitz/Cornelius*, (Fn. 2), 101 (106 f.).

153 Ausführlich *Arning/Rothkegel*, (Fn. 2), Rn. 128.

154 So auch ebd.; *Gola*, (Fn. 34), Rn. 50.

155 Vgl. *Arning/Rothkegel*, (Fn. 2), Rn. 128; *Gola*, (Fn. 34), Rn. 50.

156 Dazu ausführlich *Arning/Rothkegel*, (Fn. 2), Rn. 131.

tische Anonymisierung keine unnötigen Hürden für die Forschungsarbeit der Stellen geschaffen, die lediglich Zugang zu den pseudonymisierten Daten besitzen. Die Kombination von Pseudonymisierung und faktischer Anonymisierung gewährleistet einen angemessenen Ausgleich zwischen dem Datenschutz und der Forschungsfreiheit durch graduelle Abstufung des erforderlichen Schutzstandards.

VI. Zusammenfassung

Bei der datenschutzrechtlichen Bewertung und Einordnung der Chancen und Risiken sowie der Folgen der Anonymisierung zeigt sich zunächst, dass eine ausführliche und ausgewogene Begriffsbestimmung notwendig ist. So offenbart bereits die Bestimmung des Begriffs der Identifizierbarkeit von Daten das Grundproblem der Anonymisierung: Ist die Anonymisierung überhaupt möglich? Wenn man die Frage aus einer absoluten Sichtweise beantworten will, dann ist die Antwort: Nein. Es ist insbesondere diese Antwort, die die weitere Bewertung ausschlaggebend beeinflusst. Der Versuch aus faktischer Sicht die Frage zu beantworten, führt dazu, dass zunächst zu definieren ist, wann eine faktische Anonymisierung gegeben ist. Folglich muss in diesem Zusammenhang die Diskussion über die Zurechnung von Zusatzwissen von Dritten eröffnet werden. Es wurden drei verschiedene Ansätze dargelegt. Jedoch vermag nur der vermittelnde Ansatz zu überzeugen. Der objektive Ansatz, welcher aus dem Willen nach absoluten Ergebnissen und maximaler Rechtssicherheit folgt, führt zu nahezu unmöglichen Anforderungen für die verantwortliche Stelle. Danach wären alle Informationen als personenbezogene Daten zu behandeln, da irgendeine Stelle auf der Welt über Zusatzwissen verfügen könnte. Die Freiheitsgrundrechte werden für den maximalen Schutz des Rechts auf informationelle Selbstbestimmung eingeschränkt. Dies ist ein unverhältnismäßiges Ergebnis. Der subjektive Ansatz schafft hingegen nur im geringen Maße Abhilfe, da er sich in dem anderen Extrem verliert und ausschließlich auf den Verantwortlichen abstellt. Jedoch ist das Zusatzwissen von Dritten unter Umständen einzubeziehen. Auch deshalb ist den vom EuGH aufgestellten Parametern für die Zurechenbarkeit von Zusatzwissen zu folgen. Ohne rechtlichen Anspruch und faktische Umsetzbarkeit kann der verantwortlichen Stelle nicht das Zusatzwissen zugerechnet werden. Dieses Ergebnis ist verhältnismäßig, da es die widerstreitenden Interessen am überzeugendsten ausgleicht und den Rechtssicherheitsbedenken bzgl. des objektiven bzw. subjektiven Ansatzes entgegenwirkt.

Ferner stellt sich im Anschluss die Frage, ob die Anonymisierung auch außerhalb des Rechtsrahmens der DSGVO bestehen bleibt oder eine Datenverarbeitung i. S. d. DSGVO darstellt. Die Argumente der befürwortenden Ansicht überzeugen nicht. Der Gedanke durch eine Einordnung der Anonymisierung als Datenverarbeitung Rechtssicherheit zu schaffen, ist zwar verständlich, aber die argumentative Konstruktion dieses Ergebnisses ist dogmatisch nicht haltbar. Die intendierte Rechtssicherheit würde durch eine rechtsunsichere Lösung erschaffen werden, für die es in der Form auch keine Präzedenz gibt. Die teleologische Reduktion von Art. 9 DSGVO ist kein geeignetes Mittel die systematischen Probleme, vor die uns die Einordnung der Anonymisierung als Verarbeitung stellt, zu lösen.

Nichtsdestotrotz bleibt der rechtliche Umgang der Anonymisierung auch außerhalb der DSGVO und gerade im Anschluss an die Anonymisierung klärungsbedürftig. Die Anonymisierung stellt auf der einen Seite eine Chance für die relativ hürdenlose Nutzung und Verarbeitung von Daten in der Forschung und Wissenschaft dar. Auf der anderen Seite gilt dieser Vorteil auch für die kommerzielle Nutzung. Durch die Einordnung der Anonymisierung außerhalb der DSGVO entfallen auch Schutzmechanismen der DSGVO. Die Weitergabe an Dritte ist bspw. ohne Weiteres möglich. Dies erhöht das Risiko des Missbrauchs. Abgesehen davon, dass das Re-Identifikationsrisiko mit der Zeit, dem Zugang zu mehr Daten und dem technologischen Fortschritt steigen wird. Die Kriterien für eine Anonymisierung müssten entsprechend angepasst werden. Insbesondere für Daten besonderer Kategorien müssten hohe Anforderungen geschaffen werden. Hierbei stellt der oben dargelegte Ansatz der Konkretisierung von Anonymisierungsanforderungen im Zusammenhang mit technischen Anonymisierungsmodellen gepaart mit der für sensible Daten erforderlichen Expertenbewertung eine Lösungsmöglichkeit dar. Ergänzend dazu könnten Maßnahmen wie ein Re-Identifikationsverbot oder eine Beobachtungspflicht weiteren Schutz gewährleisten. Wobei fraglich ist, in welcher Form und unter welchem Regime die

dargestellten Anforderungen geschaffen werden könnten und ob diese Anforderungen überhaupt praktisch umsetzbar wären.

Vor diesem Hintergrund erweist sich die Pseudonymisierung als eine Art Kompromiss. Sie schafft es, die widerstreitenden Interessen des Rechts auf informationelle Selbstbestimmung und der Freiheitsgrundrechte, wie der Forschungsfreiheit, in einen ausgewogenen Einklang zu bringen. Die Pseudonymisierung ist eine Maßnahme einer datenschutzfreundlichen Voreinstellung. Die DSGVO findet weiterhin Anwendung. Insbesondere für die Forschungsvorhaben, bei denen kein Interesse daran besteht, dass die Daten vollständig anonymisiert sind, ist die Pseudonymisierung das datenschutzfreundlichste Mittel. Im Rahmen der Fremdforschung wirkt die Pseudonymisierung nach den vermittelnden Kriterien des EuGH für die Zurechenbarkeit von Zusatzwissen wie eine faktische Anonymisierung. Mithin wird ein abgestuftes Schutzregime geschaffen. Je größer der Zugang zu sensiblen Daten ist, desto höher die Anforderung an die verantwortliche Stelle.

Der Autor ist akademischer Mitarbeiter am Institut für öffentliches Recht (Abt II: Völkerrecht, Rechtsvergleichung und Rechtsethik) der Albert-Ludwigs-Universität Freiburg. Er ist dort tätig im Teilprojekt „Legal Provisions for Access and Use of Health-Related Data for Research Purposes" (Sprecherin: Prof. Dr. Silja Vöneky) des BMBF Projektes „Data Access and Data Use in Health Settings" (Sprecher: PD Dr. Joachim Boldt). Er promoviert bei Prof. Dr. Silja Vöneky zum Thema „Künstliche Intelligenz und Gesundheitsdatenschutz – Eine rechtliche und ethische Analyse der von KI-Systemen gesteuerten Verarbeitung von Gesundheitsdaten".