Stellungnahme der

TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.

zum

Konsultationspapier des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zum Thema: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche

Berlin, 23. März 2020

Korrespondenzadresse:

TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.
Charlottenstraße 42
10117 Berlin

Ansprechpartner:
Dr. Johannes Drepper, Leitung Datenschutz, IT und Qualitätsmanagement
Tel.: +49 (0)30 2200247-40,
johannes.drepper@tmf-ev.de

Über die TMF:

Die TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (kurz: TMF) ist mit gegenwärtig 64 Mitgliedern und ihren einhundert Standorten bundesweit die Dachorganisation für die medizinische Verbundforschung in Deutschland. Sie ist Plattform für den interdisziplinären Austausch und die projekt- wie standortübergreifende Zusammenarbeit, um organisatorische, rechtlich-ethische und technologische Probleme der modernen medizinischen Forschung zu identifizieren und zu lösen. Die als gemeinnützig anerkannte TMF stellt diese Lösungen frei und öffentlich zur Verfügung. Mit dem Aufbau tragfähiger Infrastrukturen für die medizinische Forschung leistet die TMF einen Beitrag zur Stärkung des Wissenschaftsstandortes Deutschland im europäischen wie internationalen Wettbewerb.

I. Zusammenfassung

Vor dem Hintergrund der hohen Relevanz der Anonymisierung von Daten in der Forschung begrüßt die TMF als Dachorganisation der medizinischen Forschung in Deutschland die Initiative des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zur Klärung der Rahmenbedingungen. In einem ersten Schritt geht es dabei nur um die rechtlichen Rahmenbedingungen, also die Anforderungen an eine Anonymisierung gemäß Erwägungsgrund Nr. 26 Datenschutz-Grundverordnung (DSGVO) und die möglichen Rechtsgrundlagen für die Anonymisierung als Verarbeitung nach Art. 4 Nr. 2 DSGVO.

Die Anonymisierung als in der DSGVO in Erwägungsgrund Nr. 26 beschriebenes Konzept anzusehen, unabhängig von dem Fehlen einer Definition in Art. 4 DSGVO, wird als sehr hilfreich angesehen. Zudem schließen wir uns der Auffassung an und halten diese für die Anwendung der Anonymisierung in der Forschung für zentral, dass neben der absoluten Anonymisierung auch eine Form der Anonymisierung den Kriterien der DSGVO entsprechen kann, bei der die Wiederherstellbarkeit des Personenbezugs nicht für alle Verarbeiter und alle Zeiten sicher ausgeschlossen werden muss. Es wäre allerdings wünschenswert, dass in dem Papier der hierfür etablierte und hilfreiche Begriff der „faktischen Anonymisierung" verwendet wird.

In Bezug auf die möglichen Rechtsgrundlagen sollte zwischen Anwendungsfällen, in denen die Ursprungsdaten bestehen bleiben, und Anwendungsfällen, in denen die Ursprungsdaten durch die anonymen Daten ersetzt werden, unterschieden werden. Denn während zweiteres auch als Teillöschung aufgefasst werden kann, ist dies für ersteres nicht der Fall.

Eine Einwilligung kann auch nach unserer Auffassung grundsätzlich für beide Anwendungsfälle als Rechtsgrundlage in Frage kommen.

Die vom BfDI vorgeschlagene Verbindung der Zweckvereinbarkeit nach Art. 5 (1) lit. b) DSGVO mit der Weitergeltung der bisherigen Rechtsgrundlage nach Art. 6 (1) oder Art. 9 (2) DSGVO wird hingegen typischerweise eher für den ersten Anwendungsfall anwendbar sein. Wir unterstützen diesen Ansatz des BfDI, sehen aber noch offene Fragen in Bezug auf die Zweckbestimmung einer Anonymisierung bzw. die Einordnung der Anonymisierung als grundsätzlich privilegierte Verarbeitung von Daten zu statistischen Zwecken. Zudem halten wir es gerade mit Blick auf die Anonymisierung als datenschutzfreundlicher Verarbeitung für zentral, dass die Weitergeltung bisheriger Rechtsgrundlagen bei vereinbaren Zwecken nach Art. 5 (1) lit. b) und Erwägungsgrund Nr. 50 Satz 2 DSGVO von den zuständigen Aufsichtsbehörden auch anerkannt wird. Der in diesem Punkt entgegengesetzt argumentierende Erfahrungsbericht der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (von der der BfDI ein Teil ist) zur Anwendung der DSGVO [1] stellt dies allerdings in Frage. Hier ist dringend eine Klärung innerhalb der Konferenz der Datenschutzbeauftragten dahingehend notwendig, dass in ganz bestimmten und eng eingegrenzten Fällen der Zweckvereinbarkeit nach Art. 5 (1) lit. b) DSGVO die

Weiterverarbeitung der Daten auf die ursprüngliche Rechtsgrundlage gestützt können werden muss. Die Anonymisierung stellt genau einen solchen vereinbaren Zweck dar und benötigt daher auch diese in der DSGVO klar angelegte Weitergeltung der ursprünglichen Rechtsgrundlage. Es ist einfach niemand zu erklären, warum man für das Zählen von Datensätzen, um ein Beispiel des BfDI aufzugreifen, eine neue und ggf. eigenständige Rechtsgrundlage benötigen soll.

Für den Anwendungsfall, bei dem die Verarbeitung personenbezogener Daten mit der Anonymisierung an ihr Ende kommt, sehen wir das Prinzip der Speicherbegrenzung nach Art. 5 (1) lit. e) DSGVO als vorrangige Rechtsgrundlage gegenüber dem vom BfDI aufgeführten Recht auf Löschen nach Art. 17 (1) DSGVO, jeweils in Verbindung mit Art. 6 (1) lit. c) DSGVO.

II. Motivation und Expertise der TMF

Die TMF – Technologie und Methodenplattform für die vernetzte medizinische Forschung (TMF) als wissenschaftlich-methodische Dachorganisation der medizinischen Forschung in Deutschland setzt sich mit den Verfahren der Anonymisierung sowie auch deren Rahmenbedingungen schon seit langem ausführlich auseinander. So diskutierte die TMF im Rahmen eines Workshops am 28.10.2014 in Berlin mit mehreren Projektpartnern und Vertretern der Arbeitskreise „Wissenschaft und Forschung" sowie „Technik" der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) ein Datenschutzkonzept zur Verarbeitung von medizinischen Routinedaten zu Forschungszwecken in der Cloud. Da hier Anonymisierungstechniken zum Einsatz kommen sollten, ging es in der Diskussion auch um den Begriff der Anonymisierung sowie mögliche Verfahren zum Anonymisieren medizinischer Daten. Nicht zuletzt der Hinweis von einigen Datenschutzbehörden in dem Workshop, dass doch für anspruchsvollere Verfahren der Anonymisierung in den Forschungseinrichtungen gar keine ausreichende Expertise vorhanden sei, führte im Nachgang der Veranstaltung dazu, dass die TMF ein umfangreiches Schulungsprogramm zur praktischen Anonymisierung medizinischer Forschungsdaten erarbeitete. Auf dieser Basis wurden in den Jahren 2016–2019 insgesamt 6 Tutorials durchgeführt, in denen toolbasiert Testdaten nach verschiedenen Methoden anonymisiert und Restrisiken der Re-Identifizierung bestimmt wurden. Alle 6 Termine waren ausgebucht. Durch diese Veranstaltungen und eine umfassende Evaluation des Schulungskonzepts konnten wichtige und hilfreiche Erfahrungen rund um das Thema der Anonymisierung medizinischer Individualdaten gesammelt werden.

In dem Workshop 2014 ging es dann aber auch um die Frage, ob denn für die Anonymisierung als Verarbeitung personenbeziehbarer Daten eine eigenständige Rechtsgrundlage notwendig ist oder nicht und wenn ja, welche möglichen Rechtsgrundlagen hierfür in der Forschung in Frage kämen. Insider verwundert es wahrscheinlich wenig, dass zu diesen Fragen im Kreise der anwesenden Vertreter von 11 Datenschutzbehörden keine Einigkeit bestand. Vor diesem Hintergrund begrüßt die TMF ausdrücklich das vom

Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) durchgeführte Konsultationsverfahren zu den Rahmenbedingungen einer Anonymisierung, auch wenn hier zunächst auf den Anwendungsbereich der Telekommunikation fokussiert wird. Ein solches Verfahren ist aus Sicht der in der TMF organisierten Forschungseinrichtungen letztlich auch mit der deutlichen Hoffnung darauf verbunden, künftig einen verlässlicheren Rahmen für die wichtige Methode der Anonymisierung in der Forschung zu haben, unabhängig davon, in welchem Bundesland und unter welcher datenschutzrechtlichen Aufsicht ein Forschungsprojekt gerade stattfindet.

III. Ziel und Gegenstand der Konsultation

In Bezug auf das Ziel und den Gegenstand der Konsultation wird in dem Papier des BfDI bereits deutlich, dass es in dem vorliegenden Konsultationsverfahren vordringlich um die rechtlichen Rahmenbedingungen und hier insbesondere um die Frage der Notwendigkeit einer Rechtsgrundlage sowie die sich daran anschließende Frage nach der Natur einer solchen Rechtsgrundlage geht. Insofern geht es hier nicht um eine Best-Practice-Anleitung dazu, wie konkret Telekommunikationsdaten anonymisiert werden können. Weder gibt es Hinweise auf die notwendige Ergebnis- noch auf die Prozessqualität in Bezug auf den Vorgang des Anonymisierens. Auch wenn die TMF solche Vorschläge zu den Methoden der Anonymisierung gerne konstruktiv aufgreifen und mit ihrer umfassenden Expertise zu diesem Thema mit Lösungskonzepten beitragen würde, sehen wir das vorliegende Konsultationsverfahren des BfDI mit der engen Beschränkung auf bestimmte rechtliche Fragen trotzdem schon als sehr hilfreich an. Zudem sind die gestellten Fragen somit auch als vergleichsweise branchenübergreifend anzusehen, auch wenn sich die Beispiele in dem Papier auf die TK-Branche beziehen. Vor diesem Hintergrund sehen wir die angesprochenen Themen auch für viele Forschungsprojekte in der Medizin als hoch relevant an und bedanken uns für die Möglichkeit der Teilnahme an diesem Konsultationsverfahren.

IV. Anforderungen an die Anonymisierung

In Bezug auf die im Positionspapier des BfDI formulierten Anforderungen an die Anonymisierung sind zwei Punkte außerordentlich zu begrüßen:

1. Die Anforderungen an eine Anonymisierung werden sehr klar aus dem Erwägungsgrund Nr. 26 der DSGVO abgeleitet. Die häufig gehörte Feststellung, die Anonymisierung sei (anders als z. B. die Pseudonymisierung) in Art. 4 DSGVO nicht definiert, ist in der Tat wenig hilfreich, zumal der Begriff der personenbezogenen Daten, der als Gegenbegriff gelten kann, sehr wohl in Art. 4 DSGVO definiert ist.
2. Aus Erwägungsgrund Nr. 26 der DSGVO wird ebenfalls sehr klar abgeleitet, dass das aus dem bis Mai 2018 anwendbaren Bundesdatenschutzgesetz bekannte Konstrukt der faktischen Anonymisierung in Ergänzung zur absoluten Anonymisierung weiterhin dem Grundsatz nach anwendbar ist. In diesem Kontext wird auch auf das Problem eingegangen, dass bei einer solchen nicht absoluten Anonymisierung, bei der die Wiederherstellung des

Personenbezugs nicht für alle Verarbeiter und alle Zeiten unmöglich sein muss, der resultierende Datensatz weiterhin zu schützen und die Eigenschaft der Anonymität fortlaufend zu validieren ist. In diesem Zusammenhang wird berechtigterweise auf die Stellungnahme der früheren Artikel-29-Gruppe zu Anonymisierungstechniken hingewiesen [2]. Es wäre allerdings wünschenswert, den bestehenden und hilfreichen Begriff der „faktischen Anonymisierung" in dem Papier der Klarheit halber auch zu verwenden.

Nicht gelöst ist allerdings das dem Datenschutzrecht bislang inhärente Problem, dass das Datenschutzrecht entweder vollständig oder gar nicht anzuwenden ist. Für faktisch anonymisierte Daten, die ggf. zu einem späteren Zeitpunkt wieder personenbeziehbar werden könnten, können daher nur untergesetzliche Normen entwickelt und angewendet werden.

V. Anonymisierung als Verarbeitung

Die Argumentation, das Anonymisieren als eine Verarbeitung gemäß Art. 4 Nr. 2 DSGVO anzusehen, ist nachvollziehbar. Wertvoll erscheint in diesem Zusammenhang auch der Hinweis aus dem Papier des BfDI, dass das Anonymisieren auf vielerlei Arten durchgeführt werden kann und z. B. auch das Zusammenfassen von personenbezogenen Daten (Aggregieren) als eine Form der Anonymisierung anzusehen ist. Insofern gehört hierzu z. B. auch das reine Zählen personenbezogener Datensätze. Dieses Beispiel macht deutlich, wie wenig invasiv der Vorgang des Anonymisierens in Bezug auf die Wahrung der Rechte und Freiheiten der betroffenen Personen ist. Das gilt insbesondere für Anonymisierungsverfahren, die automatisch, also ohne menschlichen Eingriff, durchgeführt werden können. In diesen Fällen findet somit auch keine zusätzliche Kenntnisname der personenbezogenen Daten durch einen Verarbeiter statt. Anders als bei anderen automatisierten Verarbeitungsverfahren, wie z. B. der Profilbildung, entstehen bei der automatisierten Anonymisierung auch keine neuen personenbezogenen Daten.

Die genaue Betrachtung und Einordnung dieses Sachverhalts ist deshalb so wichtig, da die Klasse der automatisierbaren Verarbeitungsvorgänge, die auf personenbezogenen Daten ablaufen und zu anonymen Ergebnissen führen, sehr groß ist und insbesondere für die Forschung erhebliches Potenzial birgt. Beispielhaft seien hier Szenarien der verteilten Auswertung medizinischer Daten mit zentraler Zusammenführung der jeweils anonymen Einzelergebnisse aller Standorte genannt, wie sie in der Medizininformatik-Initiative des BMBF[1] [3; 4] geplant sind.

VI. Rechtsgrundlagen für die Anonymisierung

Für die im Papier des BfDI diskutierten möglichen Rechtsgrundlagen ist zunächst eine Unterscheidung zwischen zwei Anwendungsfällen zu treffen, nach denen sich die Zulässigkeit der verschiedenen Rechtsgrundlagen bemisst:

[1] siehe www.medizininformatik-initiative.de

1. Die Anonymisierung findet in einer Weise statt, dass die ursprünglichen personenbezogenen Daten behalten werden. Dies kann z. B. der Fall sein, wenn nur anonyme Daten vom Verarbeiter herausgegeben oder veröffentlicht werden dürfen.
2. Die Anonymisierung stellt den Abschluss der Verarbeitung personenbezogener Daten dar. Nach der Anonymisierung sind die ursprünglichen personenbezogenen Daten nicht mehr vorhanden. Dies kann z. B. der Fall sein, wenn die Anonymisierung statt einer Löschung durchgeführt wird.

Für die in dem Papier des BfDI diskutierten Rechtsgrundlagen ist jeweils zu klären, auf welche dieser beiden unterschiedlichen Fallkonstellationen sie zutreffen können.

Einwilligung

Der Hinweis auf die Einwilligung der betroffenen Person nach Art. 6 (1) lit. a) DSGVO ist aus Sicht der Forschung gut nachvollziehbar, da in vielen Einwilligungserklärungen zu Forschungsprojekten auf die spätere Anonymisierung von Daten bereits eingegangen wird. In der TK-Branche wird diese Rechtsgrundlage mutmaßlich seltener zutreffen. Je nach Art des Forschungsprojekts und der entsprechenden Formulierung in der Einwilligungserklärung kann diese Rechtsgrundlage grundsätzlich auf beide oben skizzierten Fallkonstellationen zutreffen.

Vereinbarkeit der Zwecke und Anwendung der ursprünglichen Rechtsgrundlage

Die Prüfung der Vereinbarkeit der Zwecke nach Art. 6 (4) DSGVO in Verbindung mit der Anwendung der ursprünglichen Rechtsgrundlage erscheint uns eine gute und nachvollziehbare Grundlage für die Anonymisierung von Daten in der zweiten Fallkonstellation, wenn also die Ursprungsdaten durch die Anonymisierung nicht notwendigerweise beeinträchtigt werden. Zu dieser Auffassung sind allerdings einige Anmerkungen zu machen.

Im Rahmen der Forschung spielt die Zweckvereinbarkeit nach Art. 5 (1) lit. b) DSGVO eine besondere Rolle: „[…] eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken […]". Wie weitgehend diese Privilegierung zu verstehen ist, die zudem in Erwägungsgrund Nr. 50 DSGVO auch ohne die doppelte Verneinung aufgeführt ist, ist bis heute umstritten.

Was ist aber der datenschutzrechtlich relevante Zweck einer Anonymisierung? Kann das der Zweck sein, zu dem die anonymen Daten schließlich verwendet werden? Allerdings dürfen Daten aus Sicht des Datenschutzes grundsätzlich zu beliebigen Zwecken verwendet werden. Die datenschutzrechtliche Zweckbindung gilt nach Erwägungsgrund 26 der DSGVO für anonyme Daten nicht mehr. Insofern wäre es problematisch, als privilegierten Zweck für die Anonymisierung beispielsweise die Forschung anzugeben, wenn dann später die anonymisierten Daten zu beliebigen Zwecken verwendet werden können. Aber auch die

Annahme eines von der eigentlichen Zweckverfolgung unabhängigen Meta-Zwecks wäre nicht ganz unproblematisch.

Würde man von dem Zweck, zu dem man die anonymen Daten schließlich verwenden möchte, abstrahieren und dem Vorgang des Anonymisierens einen eigenständigen Zweck zubilligen, wäre allerdings zu fragen, was diesen eigenständigen Zweck charakterisiert. Bei genauerer Betrachtung der Anonymisierung kann man diese am ehesten als Verfahren charakterisieren, welches statistische Aussagen über einen Datensatz produziert. Hierzu sei an das bereits genannte Beispiel des Aggregierens oder Zählens der Daten erinnert (siehe Abschnitt V). Aber auch Verfahren wie die k-Anonymisierung [5] stellen im Prinzip eine Vergröberung von Individualdaten nach bestimmten statistischen Kriterien dar. In aller Regel könnte man die Anonymisierung insofern als eine Art der statistischen Verarbeitung der Daten darstellen bzw. im Sinne der DSGVO hier statistische Zwecke als anderen Zwecken vorgeordnet annehmen. Somit könnte bei der Prüfung der Vereinbarkeit der Zwecke auch jenseits einer anzunehmenden Privilegierung der Forschung von einer allgemeinen Privilegierung der Anonymisierung ausgegangen werden, wenn diese statistischen Zwecken dient. Dazu passt auch, dass Roßnagel den Grund der Privilegierung der in Art. 5 (1) lit. b) DSGVO genannten Zwecke gerade darin sieht, dass sich diese typischerweise nicht auf die Person zu einem Datensatz beziehen [6, Art. 5 Rn. 104]. Dass sich der anonyme Datensatz nicht mehr auf einzelne Personen beziehen lässt, ist aber gerade das Definitionskriterium der Anonymität.

Kontrovers diskutiert wird, auf welche Rechtsgrundlage eine Verarbeitung bei Vereinbarkeit der Zwecke gestützt werden kann. Unter Verweis auf Erwägungsgrund Nr. 50 Satz 2 DSGVO soll dies nach dem BfDI die ursprüngliche Rechtsgrundlage der Datenverarbeitung sein. Jede Rechtsgrundlage einer Datenverarbeitung unterliegt demnach dem Prinzip der Zweckbindung (Art. 5 (1) lit. b) DSGVO), zu dem aber auch gehört, dass die Verarbeitung zu vereinbaren Zwecken in engen Grenzen von der ursprünglichen Rechtsgrundlage mit abgedeckt ist. Dieser Sichtweise schließen wir uns hier ausdrücklich an (vergl. dazu auch Roßnagel in [6, Art. 5 Rn. 98]).

Die z. T. auch vertretene Gegenmeinung (vergl. etwa [7, S. 1844]), dass für vereinbare Zwecke eine neue bzw. eigenständige Rechtsgrundlage gelten muss, würde hingegen bedeuten, dass sich aus der Zweckvereinbarkeit eine zusätzliche Einschränkung in Bezug auf die möglichen Rechtsgrundlagen ergäbe. Trotz vorhandener, neuer Rechtsgrundlage könnte dann eine Weiterverarbeitung von Daten ggf. mangels Zweckvereinbarkeit nicht zulässig sein. Da die Zweckvereinbarkeit in Art. 6 (4) im Vergleich zu den Rechtsgrundlagen in Art. 6 (1) und in Art. 9 (2) DSGVO sehr viel unschärfer definiert ist, würde sich daraus eine erhebliche Rechtsunsicherheit in Bezug auf die rechtmäßige Verarbeitung personenbezogener Daten ergeben.

Für die Geltung der ursprünglichen Rechtsgrundlage für vereinbare Zwecke bei der Weiterverarbeitung personenbezogener Daten sprechen auch weitere, in der DSGVO angelegte Privilegierungen, die sich sonst kaum innerhalb des Prinzips der Rechtmäßigkeit

nach Art. 6 (1) DSGVO abbilden ließen. Hierzu gehört die in Art. 5 (1) lit. e) festgelegte Erlaubnis, dass Daten für bestimmte privilegierte Zwecke auch länger in personenbeziehbarer Form gespeichert werden dürfen. In eine ähnliche Richtung geht zudem die Privilegierung in Art. 17 (3) lit. d), die das Recht auf Löschung bei einer Verarbeitung für bestimmte Zwecke einschränkt. In beiden Fällen kann eigentlich sinnvollerweise nur die Weitergeltung der ursprünglichen Rechtsgrundlage angenommen werden, insbesondere wenn man vor dem Hintergrund der engen und abschließenden Formulierungen in Art. 6 (1) und Art. 9 (2) DSGVO davon absieht, dass Art. 5 (1) lit. e) und Art. 17 (3) lit. d) eigenständige Rechtsgrundlagen darstellen könnten.

Die ausführliche Argumentation für die Weitergeltung der bisherigen Rechtsgrundlage bei einer Weiterverarbeitung zu vereinbaren Zwecken ist hier leider notwendig, da die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) im November 2019 und unter Beteiligung des BfDI einen Erfahrungsbericht zur Anwendung der DSGVO vorgelegt hat, in dem diese Weitergeltung explizit problematisiert und die Streichung des hierfür scheinbar zentralen zweiten Satzes in Erwägungsgrund Nr. 50 DSGVO gefordert wird [1, S. 13f]. Übersehen wird dabei, dass die Weitergeltung der bisherigen Rechtsgrundlage in der DSGVO implizit tiefer verankert ist, als es auf den ersten Blick scheint. Nicht nur würde den oben schon genannten Regelungen in Art. 5 (1) lit. e) und Art. 17 (3) lit. d) DSGVO ohne Weitergeltung der bisherigen Rechtsgrundlage sozusagen „der Boden entzogen"; auch Erwägungsgrund Nr. 50 Satz 5 bestätigt den Grundsatz der möglichen Weitergeltung: „Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung dienen."

Insofern plädieren wir hier sehr deutlich für den im Papier des BfDI zur Anonymisierung dargestellten Ansatz, für die Anonymisierung eine mögliche Rechtsgrundlage darin zu sehen, dass eine Vereinbarkeit der Zwecke nach Art. 6 (4) bestehen kann und dann von einer Weitergeltung der ursprünglichen Rechtsgrundlage auszugehen ist. Die diesbezügliche Sichtweise der DSK [1, S. 13f], die sicher nicht ohne Beteiligung des BfDI entstanden sein wird, lehnen wir hingegen strikt ab, auch wenn der Erfahrungsbericht der DSK zu anderen Problemen im Umgang mit der DSGVO viele positive Ansätze und Überlegungen enthält.

Gesetzliche Verpflichtung in Verbindung mit dem Recht auf Löschung

Als weitere mögliche Rechtsgrundlage für eine Anonymisierung wird die gesetzliche Verpflichtung des Verantwortlichen nach Art. 6 (1) lit. c) DSGVO in Verbindung damit gesehen, dass ein Betroffener sein Recht auf Löschung nach Art. 17 (1) DSGVO geltend macht. Diese Rechtsgrundlage ist zunächst alleinig auf die oben beschriebene Fallkonstellation Nr. 2 anwendbar, wenn also nach dem Vorgang der Anonymisierung die personenbeziehbaren Ursprungsdaten tatsächlich nicht mehr vorhanden sind. Viel grundlegender als das sehr öffentlichkeitswirksam mit der DSGVO neu eingeführte „Recht auf Vergessenwerden" (Art. 17 DSGVO) wirken aber im Datenschutzrecht die viel älteren Prinzipien der Erforderlichkeit bzw. der „Speicherbegrenzung" (Art. 5 (1) lit. e) DSGVO). So

statuiert Art. 5 (1) lit. e) DSGVO, dass bei einer Speicherung von Daten die Identifizierung der betroffenen Personen nur so lange möglich sein soll, „wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist". Schon aus diesem Grundsatz lässt sich eine gesetzliche Verpflichtung nach Art. 6 (1) lit. c) DSGVO ableiten, personenbezogene Daten, wenn sie nicht mehr benötigt werden oder der Personenbezug nicht mehr benötigt wird, zu löschen bzw. zu anonymisieren. Diese gesetzliche Verpflichtung besteht auch völlig unabhängig davon, ob ein Betroffener nach Art. 17 (1) DSGVO sein Recht auf Löschung geltend macht oder nicht. Insofern sollte die Kombination aus Art. 5 (1) lit. e) in Verbindung mit Art. 6 (1) lit. c) DSGVO in das Positionspapier noch vor der Kombination mit Art. 17 (1) DSGVO aufgenommen werden.

Die Frage, ob eine Anonymisierung auch eine nach Art. 17 (1) DSGVO verlangte Löschung ersetzen kann, wird in dem Papier des BfDI in der aktuellen Fassung bejaht, was aus praktischer Sicht und mit Blick auf die eigentlich hier nicht zur Diskussion stehenden Anwendungsfälle in der medizinischen Forschung sehr zu begrüßen ist. Gleichwohl können wir derzeit nicht übersehen, ob diese Ansicht mehrheitlich von den deutschen Aufsichtsbehörden geteilt wird und somit als Basis einer entsprechenden Empfehlung trägt.

VII. Anhang

Literatur

1. DSK *Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO*. 2019. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder - Datenschutzkonferenz (DSK), November 2019, https://www.datenschutzkonferenz-online.de/media/dskb/20191213_erfahrungsbericht_zur_anwendung_der_ds-gvo.pdf (Abruf: 2020-02-27).

2. Artikel-29-WP *Opinion 05/2014 on Anonymisation Techniques*. 2014. Article 29 Data Protection Working Party, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (Abruf: 2020-03-23).

3. Semler, S.C., *Die Medizininformatik-Initiative als Impulsgeber für Standardisierung und Datennutzung im deutschen Gesundheitswesen.* mdi, 2019. **2019**(4): S. 96-98.

4. Hemmer, B., Börries, M., Christoph, J., Marx, G., Maaßen, O., Schuppert, A., Scheithauer, S., *Die klinischen Anwendungsbeispiele (Use Cases) der vier MII-Konsortien.* mdi, 2019. **2019**(4): S. 98-102.

5. Sweeney, L., *k-Anonymity: A model for protecting privacy.* International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002. **10**(05): S. 557 - 570.

6. Simitis, S., Hornung, G., Spiecker gen. Döhmann, I., Hrsg. *Datenschutzrecht. DSGVO mit BDSG. Großkommentar*. 1. Aufl. 2019, Nomos, Baden-Baden.

7. Schantz, P., *Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht.* Neue Juristische Wochenschrift, 2016. **2016**(26): S. 1841-1904.

Abkürzungen

BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (www.bfdi.bund.de)
DSGVO	Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (Verordnung 2016/679)
DS-GVO	siehe DSGVO
DSK	Datenschutzkonferenz – Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (www.datenschutzkonferenz-online.de)
EG	Europäische Gemeinschaft
TK	Telekommunikation
TMF	TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (www.tmf-ev.de)
WP	Working Party der Europäischen Arbeitsgruppe zum Datenschutz gemäß Artikel 29 der Richtlinie 95/46/EG