”Legal map” of the applicable legal framework conditions for research data processing

Authors:

Lettieri, Vanessa[1]; Kipker, Dennis-Kenji[1]; Buchner, Benedikt[1]

on behalf of the NFDI4Health Consortium

Acknowledgement:

Ahrens, Wolfgang[2]; Drepper, Johannes[3]; Fluck, Juliane[5]; Fröhlich, Holger[4]; Gehrke, Juliane[3]; Goek Ng, Hwei[4]; Haber, Anna C.[6]; Henke, Christian[7]; Holick, Marcel[3]; Intemann, Timm[2]; Kaulke, Knut[3]; Kirsten, Toralf; Kuntz, Alessandra S.[7]; Prasser, Fabian[6]; Sax, Ulrich[7]; Semler, Sebastian[3];

[1] University of Bremen / University of Augsburg (since 01/08/2022)
[2] Leibniz Institute for Prevention Research and Epidemiology – BIPS
[3] Technology, Methods, and Infrastructure for Networked Medical Research – TMF
[4] Fraunhofer Institute for Algorithms & Scientific Computing – SCAI
[5] Information Centre for Life Sciences – ZB MED
[6] Berlin Institute of Health at Charité – Universitätsmedizin Berlin
[7] Georg-August University Göttingen, University Medical Center (Institute for Medical Informatics)

DOI: 10.4126/FRL01-006449528

Version: V1_0

Publication date: 20.06.2023

This work was done as part of the NFDI4Health Consortium (www.nfdi4health.de). We gratefully acknowledge the financial support of the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – project number 442326535.

D6.2 - “Legal map” of the applicable legal framework conditions for research data processing

Inhalt

A. Einführung, Hintergrund und Zielsetzung

Datenschutz und wissenschaftliche Forschung stehen zueinander nicht selten in einem Spannungsverhältnis[1]: Einerseits sollen durch die Forschung Gemeinwohlbelange gefördert werden – beispielsweise mit Blick auf die Forschung zur Eindämmung des Coronavirus – andererseits entbindet auch das datenschutzrechtliche Forschungsprivileg nicht von einer datenschutzrechtlichen Verantwortlichkeit der forschenden Einrichtung.

Somit sind auch im Rahmen der wissenschaftlichen Forschung für die Verwendung von Daten wie beispielsweise Gesundheits- und Sozialdaten umfassende datenschutzrechtliche Vorgaben zu beachten. Die Nutzung einzelner sowie die Verknüpfung unterschiedlicher Datenquellen (insb. Primär- und Sekundärdaten) unterliegt einem komplexen datenschutzrechtlichen Regelungsregime, das überdies Besonderheiten im Hinblick auf die wissenschaftliche Forschung enthält, in deren Rahmen sich deshalb auch besondere organisatorische Herausforderungen stellen.[2] Zwar enthält die DS-GVO zahlreiche Erleichterungen für die Forschung, ungeachtet dessen bestehen in der Forschungspraxis aber weiterhin erhebliche Unklarheiten über die Anwendung und Auslegung der Regelungen und somit deren Reichweite im konkreten Fall.[3] Erschwerend hinzu tritt, dass die Vorschriften auf unterschiedlichen Regulierungsebenen angesiedelt und teils allgemeiner, teils bereichsspezifischer Natur sind, sodass sich in Gesamtbetrachtung ein kompliziertes Rahmenwerk ergibt.

Die vorliegende Deliverable D6.2 stellt den Status quo der datenschutzrechtlichen Rahmenbedingungen für die Forschung im Allgemeinen und für das Record Linkage im Rahmen von NFDI4Health im Besonderen dar, indem die Legitimationsgrundlagen der Datenverarbeitung für Forschungszwecke aus den unterschiedlichen Regelungen aus dem Europa-, Bundes- und Landesrecht in einer „Legal Map“ systematisiert aufgearbeitet werden.

B. Anwendungsbereich des EU-Datenschutzrechts

Im ersten Schritt einer juristischen Betrachtung des Datenschutzrahmens in der Forschung ist der Anwendungsbereich des jeweiligen Rechtsaktes zu bestimmen. Der Ausgangspunkt stellt dabei das europäische Datenschutzrecht, also die Datenschutz-Grundverordnung (DS-GVO) dar.

Grundsätzlich gilt die DS-GVO als europäische Verordnung unmittelbar in allen Mitgliedstaaten.[4] Allerdings bestimmen zahlreiche bereichsspezifische Öffnungsklauseln innerhalb der DS-GVO, dass die Mitgliedstaaten nationale Regelungen erlassen können, die den Datenschutz in Einklang mit der Verordnung

[1] *Roßnagel*, ZD 2019, 157.
[2] Vgl. *March et al.*, FDZ-Methodenreport 12/2015, 3.
[3] *Cepic*, ZD-Aktuell 2021, 05214.
[4] *Weichert,* Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, S. 27.

abgestufter regeln, um nationalen Besonderheiten z.B. in der Sozialverwaltung angemessen Rechnung zu tragen. Soweit die Mitgliedstaaten von Öffnungsklauseln Gebrauch gemacht haben, haben die entsprechenden nationalen Regelungen Vorrang vor der Anwendung der DS-GVO.[5]

I. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich der DS-GVO ist gem. Art. 2 eröffnet, wenn eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten erfolgt. Eine Verarbeitung im Sinne der DS-GVO umfasst jede Handlung im Zusammenhang mit personenbezogenen Daten, namentlich verändern, speichern, übermitteln, erheben, löschen, verknüpfen. Der Begriff der Datenverarbeitung ist somit weit gefasst und es kommt nicht auf den Umfang oder die Dauer einer Datenverarbeitung an.[6] Eine Besonderheit ist darin zu sehen, dass die Datenverarbeitung zu Forschungszwecken nicht selten auf die Verarbeitung von besonderen Kategorien personenbezogener Daten abzielt, wozu gem. Art. 9 Abs. 1 DS-GVO nicht nur Gesundheitsdaten, sondern auch genetische und biometrische Daten sowie Sexualdaten zu zählen sind.

II. Personenbezogene Daten

Die Anwendbarkeit des Datenschutzrechts setzt stets das Vorliegen personenbezogener Daten voraus. Personenbezogene Daten sind gem. Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, die sog. „betroffene Person“, beziehen. Zu unterscheiden ist somit zwischen der Datenverarbeitung basierend auf personenidentifizierenden Merkmalen und der Datenverarbeitung, die keine personenidentifizierenden Merkmale verwendet. Identifizierbar ist eine Person gem. Art. 4 Nr. 1 DS-GVO dann, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung (Namen, Kennnummer etc.) oder sonstigen besonderen Merkmalen, wozu auch physische, physiologische, genetische, psychische und soziale Merkmale gehören können, identifiziert werden kann. Zur Beurteilung der Identifizierbarkeit einer natürlichen Person sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine natürliche Person zu identifizieren bzw. um sie auszusondern. Hierbei kommt es auf die wahrscheinlich als Identifizierungsmittel genutzten Ressourcen an, wozu Kosten, Zeitaufwand und Technologie gehören können.[7] Insbesondere dann, wenn miteinander kombinierte Informationen den Rückschluss auf eine Einzelperson zulassen, kann von personenbezogenen Daten gesprochen werden.[8]

---

[5] *Roßnagel*, ZD 2019, 157, 159.
[6] *Ernst,* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO, Rn. 20.
[7] *Schild*, in: BeckOK-Datenschutzrecht, Art. 4 DS-GVO, Rn. 15.
[8] *Ernst,* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO, Rn. 13.

III. Pseudonymisierte und anonymisierte Daten

Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken unterliegt gem. Art. 89 Abs. 1 S. 1 DS-GVO „geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person". Der Grundsatz der Datenminimierung sowie die Wahrung der Rechte und Freiheiten betroffener Personen sollen durch technische und organisatorische Maßnahmen sichergestellt werden. Im Hinblick auf diese Maßnahmen nennt Art. 89 Abs. 1 S. 3 DS-GVO die Pseudonymisierung. Die Anonymisierung wird in dieser Vorschrift nicht explizit genannt, der Erwägungsgrund 26 der Verordnung legt dahingehend aber fest, dass die DS-GVO nicht für „anonyme Informationen" gilt.

Im Folgenden wird auf das begriffliche Verständnis von pseudonymisierten und anonymisieren Daten im Sinne des europäischen Datenschutzrechts eingegangen.

1. Pseudonymisierte Daten

Die Pseudonymisierung von personenbezogenen Daten ist in Art. 4 Nr. 5 legaldefiniert als die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Dazu müssen die zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten einer identifizierten oder identifizierbaren natürlichen Person nicht zugewiesen werden. Die Pseudonymisierung wird etwa bei wissenschaftlichen Studien genutzt, wenn es von Bedeutung ist, den einzelnen Probanden für Rückfragen oder eventuell festgestellte Krankheitsbilder und Diagnosen kontaktieren zu können.[9] Zu beachten ist, dass es sich bei pseudonymisierten Daten weiterhin um personenbezogene Daten handelt,[10] sodass der Anwendungsbereich des Datenschutzes nach wie vor vollständig eröffnet ist. Jedoch stellt die Pseudonymisierung eine technisch-organisatorische Maßnahme (TOM) dar, um Datensparsamkeit und Datensicherheit gem. Art. 32 DS-GVO zu realisieren.

2. Anonymisierte Daten

Gem. Art. 2 Abs. 1 DS-GVO ist der Anwendungsbereich des Datenschutzrechts eröffnet, soweit eine Verarbeitung personenbezogener Daten erfolgt. Bei personenbezogenen Daten handelt es sich nach der Legaldefinition in Art. 4 Nr. 1 DS-GVO um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Erwägungsgrund 26 der DS-GVO stellt klar, dass das Gesetz auf

[9] *Weichert*, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 125.
[10] *Schild,* in: BeckOK-Datenschutzrecht, Art. 4 DS-GVO, Rn. 78.

anonymisierte Daten hingegen keine Anwendung findet. Auch wenn die Anonymisierung begrifflich erwähnt und auch an verschiedenen Stellen der DS-GVO vorausgesetzt wird, wird sie durch das Gesetz nicht legaldefiniert[11] und ist nur rudimentär geregelt.[12] Allgemein versteht man unter Anonymisierung das Verändern personenbezogener Daten derart, 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.[13] Der Anonymisierungsvorgang als solcher ist dabei jedoch als eine Datenverarbeitung anzusehen und unterfällt deshalb dem Anwendungsbereich der DS-GVO, sodass er einer Rechtfertigung bedarf.[14]

Entscheidend zur Beurteilung der Anonymisierung ist die Frage, ab wann eine Person nicht mehr als identifizierbar einzuordnen ist. Nach Erwägungsgrund 26 der DS-GVO sollen dafür alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden. Maßgeblich für diese Bewertung ist stets der Zeitpunkt der Verarbeitung.[15] Umstritten ist jedoch, auf welches Zusatzwissen abzustellen ist, konkret ob auch das etwaige Wissen anderer Personen zur Identifizierung berücksichtigt werden muss. Unterschieden wird zwischen dem **absoluten Ansatz**, wonach die Zuordnung einer Einzelangabe zu einer konkreten Person für jedermann unmöglich sein muss,[16] sowie dem **relativen Ansatz**, wonach lediglich die Mittel zu berücksichtigen sind, die der jeweiligen verantwortlichen Stelle tatsächlich und im konkreten Einzelfall zur Verfügung stehen, um den Personenbezug festzustellen (sog. „faktische Anonymität").[17]

Umstritten ist, ob eine Anonymisierung voraussetzt, dass die Re-Identifizierung unmöglich ist. Zum Teil wird vertreten, dass im Fall einer solchen Wiederherstellung des Personenbezugs nur von einer Pseudonymisierung auszugehen sein wird, so dass durchgängig personenbezogene Daten anzunehmen wären.[18] Auch die Art.-29-Datenschutzgruppe ging in einer Stellungnahme aus dem Jahr 2014 noch davon aus, dass eine Anonymisierung voraussetzt, dass eine Identifizierung unwiderruflich unmöglich wird.[19]

Mittlerweile dürfte aber davon auszugehen sein, dass es in Anbetracht der sich laufend weiterentwickelnden technischen Möglichkeiten keine absolute und unumstößliche Anonymität von Daten mehr geben

[11] *Roßnagel*, ZD 2021, 188, 189.
[12] *BfDI*, Positionspapier zur Anonymisierung, 2.
[13] *Roßnagel*, ZD 2021, 188, 189 mit Verweis auf die entsprechenden Definitionen in den landesgesetzlichen Regelungen; *Ernst,* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO Rn. 48.
[14] *Roßnagel*, ZD 2021, 188, 189.
[15] *Klar/Kühling,* in: Kühling/Buchner, DS-GVO BDSG, Art. 4 Abs. 1 DS-GVO, Rn. 24 mwN.
[16] *Schmidt,* in: Taeger/Gabel, DS-GVO BDSG, Art. 2 DS-GVO, Rn. 7.
[17] *Karg* in, Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 1 DS-GVO, Rn. 59 mwN.
[18] So *Ernst,* in: Paal/Pauly, DS-GVO BDSG, Art. 4, Rn. 49.
[19] *Art.-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, 0829/14/DE WP 216, S. 3.

kann.[20] Diese Erkenntnis entspricht dem Ansatz des relativen Personenbezugs, dass vielmehr eine Risikoprognose vorzunehmen ist. Auch die EuGH-Entscheidung Breyer / Deutschland (Urt. v. 18.10.2016 – Rn. C-582) kann im Sinne der relativen Theorie verstanden werden, die nicht zuletzt auch in der Literatur weit verbreitet ist.[21] Wird im Rahmen der Risikoprognose ermittelt, dass der Aufwand zur Re-Identifizierung dermaßen unverhältnismäßig ist, dass eine solche nach allgemeiner Lebenserfahrung und dem Stand von Wissenschaft und Technik nicht zu erwarten ist, ist ein Personenbezug nach dem relativen Ansatz abzulehnen. In die Risikoprognose einzubeziehen sind auch „das vorhandene oder erwerbbare Zusatzwissen des Verantwortlichen, aktuelle und künftige technische Möglichkeiten der Verarbeitung sowie der mögliche Aufwand und die verfügbare Zeit".[22] Diesbezüglich wird es nach dem relativen Ansatz jedoch als ausreichend erachtet, „wenn zum Zeitpunkt der Anonymisierung vernünftigerweise ausgeschlossen ist, dass der Verantwortliche mit dem ihm verfügbaren oder absehbar erwerbbaren Zusatzwissen eine Zuordnung der Daten zur betroffenen Person vornehmen kann".[23] Dem relativen Ansatz folgend kommt es zur Beurteilung der Anonymisierung damit entscheidend darauf an, ob es absehbar ist, dass der Personenbezug der Forschungsdaten wiederhergestellt wird.

Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) schlägt argumentativ wohl einen ähnlichen Weg ein, wenn er in seinem „Positionspapier zur Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche" aus Juni 2020 feststellt, dass für eine Anonymisierung nicht gefordert wird, dass der Personenbezug von niemandem mehr hergestellt werden kann. Ausreichend sei in der Regel, dass eine Re-Identifizierung praktisch nicht durchführbar ist.[24]

Unter allen Umständen der heutzutage vernetzten Datenverarbeitung noch eine absolute Anonymisierung zu verlangen, setzt im Ergebnis nicht nur der technischen Entwicklung erhebliche Hindernisse entgegen, sondern würde auch Vorgaben schaffen, die in der Realität vielfach nicht umzusetzen sind – dies gilt insbesondere auch mit Blick auf komplexe Forschungsvorhaben. Daher wird zu Recht vertreten, dass die Vorstellung einer absoluten Anonymisierung gegenüber der technischen Entwicklung und damit der Wirklichkeit zurückbleibt.[25]

Zu beachten ist jedoch zusätzlich, dass selbst wenn eine Anonymität der verarbeiteten Daten angenommen wird, dennoch datenschutzrechtliche Pflichten fortbestehen, da der Datenschutz auch vor einer mög-

[20] Vgl. auch *Hackenberg*, in: Handbuch Multimedia-Recht, Teil 15.2, Rn. 53: „Soweit das BDSG von der Vorstellung ausgeht, dass es eine absolute Anonymisierung gäbe, bleibt diese Vorstellung wohl hinter der technischen Wirklichkeit zurück."; ähnlich auch *Roßnagel*, ZD 2021, 188, 189: „Ein absoluter Ausschluss der Zuordnung ist weder möglich noch erforderlich."
[21] Siehe u.a. *Ziebarth,* in: Sydow, DS-GVO, Art. 4, Rn. 29 f.
[22] *Roßnagel/Geminn*, ZD 2021, 487, 488.
[23] *Roßnagel*, ZD 2021, 188, 191.
[24] *BfDI,* Positionspapier zur Anonymisierung, 4.
[25] *Hackenberg,* in: Hoeren/Sieber/Holznagel, Handbuch-Multimedia-Recht, Teil 15.2, Rn. 53.

lichen De-Anonymisierung von Datenbeständen schützt. Daher müssen solche notwendigen Maßnahmen ergriffen werden, die dieses Risiko weitestgehend möglich reduzieren oder bestenfalls verhindern. Hierzu gehört beispielsweise nicht nur die Wahl eines hinreichend sicheren technischen Verfahrens zur Datenanonymisierung, sondern ebenso die fortlaufende Beobachtung und Berücksichtigung der technischen Entwicklung. Zu prüfen ist insbesondere, ob – gegebenenfalls durch außerordentliche Umstände – durch Zeitablauf technische Schwachstellen im Anonymisierungsverfahren auftreten können. Ebenso zu erwägen sind automatische Löschkonzepte für Daten, die nicht mehr benötigt werden bzw. deren weitere Verarbeitung durch Zeitablauf obsolet wird. Dies entspricht ebenso der Auffassung des BfDI, wenn er annimmt, dass es trotz einer Anonymisierung die Aufgabe des Verantwortlichen bleibt, die Überprüfung der Anonymisierung auf ihre Validität fortwährend durchzuführen. Dies wird entsprechend durch die Datenschutzaufsicht überwacht.[26]

Mit Blick auf das Re-Identifizierungsrisiko von Forschungsdaten gilt bei der Verarbeitung von Gesundheitsdaten eine Besonderheit: So ist zu beachten, dass je seltener ein Krankheitsbild und je kleiner eine Probandengruppe ist, umso weniger von anonymen Datensätzen ausgegangen werden kann, da sich gerade bei kleinen Personengruppen mit seltenen Erkrankungen das Re-Identifizierungsrisiko signifikant erhöhen dürfte.[27]

Überdies kann auch mit Blick auf die Wertungen des relativen Ansatzes eine grundsätzlich zu begrüßende Anonymisierung von Forschungsdatensätzen vor allem daran scheitern, dass eine technisch wie rechtlich sichere Anonymisierung in Zeiten von KI-gestützter Datenverarbeitung, Big Data, Data Warehousing und Co. immer schwieriger zu realisieren ist. Bevor sich eine Forschungseinrichtung deshalb auf die Anonymität eines Datensatzes beruft, ist dieser zuvor genauestens zu überprüfen und unter den zuvor angestellten rechtlichen Erwägungen im Einzelfall zu bewerten.

IV. Synthetische Daten

Eine Datenverarbeitungstechnologie eröffnet aktuell interessante datenschutzrechtliche Perspektiven für den Forschungsbereich: Bei der Synthetisierung von Daten wird ein KI-gestützter Lernalgorithmus dazu verwendet, um aus Original-Patientendaten realistisch simulierte Daten zu generieren. Diese werden auch als „synthetische Daten“ bezeichnet. Hierzu werden in dem technischen Verfahren die statistischen Informationen und Strukturen eines echten Datensatzes maschinell erlernt und mithilfe des Algorithmus „synthetisiert“.[28]

---

[26] *BfDI*, Positionspapier zur Anonymisierung, 4.
[27] *Conrad/Treeger,* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 34, Rn. 106.
[28] *Wegner* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 6.5, Rn. 1 ff.

Für die Forschung stellt sich die Frage, ob es sich bei der Generierung von synthetischen Daten um eine Anonymisierungstechnik handelt mit der zuvor skizzierten Folge, dass die wissenschaftliche Verarbeitungstätigkeit mangels Eröffnung des sachlichen Anwendungsbereichs nicht mehr den strengen Beschränkungen der DS-GVO unterliegt.[29]

Zu berücksichtigen dabei ist, dass für das Verfahren zur Herstellung synthetischer Datensätze die personenbezogenen Forschungsdaten nicht lediglich um Identifikationsmerkmale entsprechend einer Anonymisierungstechnologie bereinigt werden, sondern technisch ein komplett neuer Datensatz erzeugt wird, der auf dem trainierten Verständnis eines Originaldatensatzes basiert. Fraglich ist, ob der fertige synthetische Datensatz die datenschutzrechtlichen Anforderungen der Anonymisierung erfüllt.

Zur Herstellung synthetischer Daten sind mit Blick auf die Anonymisierung verschiedene Faktoren zu berücksichtigen: so zum einen die Ausgestaltung des Originaldatensatzes, der mindestens in pseudonymisierter oder anonymisierter Form in den Algorithmus eingepflegt wird; zum anderen die bei der Datenverarbeitung zugrunde gelegten technisch-organisatorischen Maßnahmen. Darüber hinaus ist zu berücksichtigen, dass die generierten synthetischen Daten nicht „frei in die Welt übermittelt werden", sondern dazu dienen, die Daten einem bestimmten Nutzerkreis mit einem bestimmten Forschungsinteresse einfacher zugänglich zu machen.

Gemessen an den vorangehend dargestellten rechtlichen Anforderungen ist die Frage der Anonymisierung durch die Generierung von synthetischen Daten anhand einer Risikoprognose zu klären, in deren Rahmen die Wahrscheinlichkeit eines Re-Identifizierungsrisikos unter Verhältnismäßigkeitsgesichtspunkten zu prüfen und bewerten ist.[30] Für die Feststellung und Bestimmbarkeit der Wahrscheinlichkeit eines derartigen Re-Identifizierungsrisikos muss die zum Zeitpunkt der Verarbeitung verfügbare Technologie als auch die weitere technologische Entwicklung betrachtet werden (Erwägungsgrund 26 DS-GVO), da ein technisches Verfahren, das aktuell eine Anonymisierung garantiert, ein vergleichbares Schutzniveau in der Zukunft möglicherweise nicht mehr gewährleisten könnte. [31] Dabei sind neben den technologischen Faktoren ebenso wirtschaftliche Aspekte in die Bewertung einzubeziehen.[32] Die Datenverarbeitung zur Durchführung einer Anonymisierung muss folglich eine technische „Schutzreserve" beinhalten, die den erweiterten Risiken zukünftiger Technologieentwicklung vorbeugt.[33]

Im Ergebnis dürfte es durch das vorangehend beschriebene technische Verfahren zur synthetischen Datenherstellung grundsätzlich nicht mehr oder nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten,

[29] Vgl. *Ernst,* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO, Rn. 48; *Schild*, in: BeckOK-Datenschutzrecht, Art. 4 DS-GVO, Rn. 27b.
[30] *Bischoff*, PharmR 2020, 309, 312 f.; *Schild*, in: BeckOK-Datenschutzrecht, Art. 4 DS-GVO, Rn. 27b.
[31] *Ernst,* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO, Rn. 9.
[32] *Klabunde,* in: Ehmann/Selmayr, DS-GVO, Art. 4 Rn. 17.
[33] *Schaar*, ZD 2016, 224, 225.

Know-How und Arbeitskraft möglich sein, einen Personenbezug herzustellen. Dem relativen Ansatz der Anonymisierung folgend würde daher auch eine entsprechende Risikoprognose ergeben, dass der Aufwand zur Re-Identifizierung regelmäßig derart unverhältnismäßig sein wird, dass eine solche nach allgemeiner Lebenserfahrung und dem Stand von Wissenschaft und Technik nicht zu erwarten ist. So dürfte es zum Zeitpunkt der Synthetisierung bzw. Anonymisierung der Daten, auf den bei der rechtlichen Betrachtung abzustellen ist, vernünftigerweise ausgeschlossen sein, dass der Verantwortliche mit dem ihm verfügbaren oder absehbar erwerbbaren Zusatzwissen eine Zuordnung der Daten zur betroffenen Person vornehmen kann.

Der Umgang mit synthetischen Daten und deren datenschutzrechtliche Bewertung im Einzelnen ist rechtswissenschaftlich gegenwärtig jedoch noch weitestgehend unerforscht, ebenso existiert keine gerichtliche oder aufsichtsbehördliche Anwendungs- und Auslegungspraxis. Daher kann für die Anonymität synthetischer Daten keine generelle Aussage getroffen werden, sondern es muss eine auf den konkreten Einzelfall zugeschnittene rechtliche Bewertung des technischen Sachverhalts erfolgen.

C. Verarbeitungsgrundsätze für den Umgang mit personenbezogenen Daten im Kontext der wissenschaftlichen Forschung

Die DS-GVO bestimmt zentrale Prinzipien, nach denen sich jede Verarbeitung von personenbezogenen Daten – auch im Forschungskontext – richten muss. Diese Prinzipien werden teils ausdrücklich im Gesetz benannt, teils aus rechtlichen Anforderungen mittelbar abgeleitet. Der Verantwortliche einer Datenverarbeitung muss die Einhaltung dieser Grundsätze beachten und ist gem. Art. 5 Abs. 2 DS-GVO für diese nachweispflichtig.

Infolge der strengen datenschutzrechtlichen Vorgaben kann es zu Konflikten mit der Forschungsfreiheit kommen, da diese es nicht selten erfordert, dass umfassende personenbezogene Datenbestände verarbeitet werden.[34] Deshalb sieht die DS-GVO für die wissenschaftliche Forschung Privilegien vor, die die Verarbeitung von personenbezogenen Daten einerseits erleichtern, andererseits aber ebenso Garantien für die Rechte und Freiheiten der betroffenen Personen als Ausgleich für die gewährten Erleichterungen fordern, die sich aus den Verarbeitungsgrundsätzen für den Umgang mit personenbezogenen Daten ergeben können.[35]

[34] *Stender-Vorwachs,* in: BeckOK-Datenschutzrecht, Art. 85 DS-GVO, Rn. 24.
[35] *Roßnagel*, ZD 2019, 157, 157 ff.

I. Verbotsprinzip (mit Erlaubnisvorbehalt)

Zentraler Grundsatz und Ausgangspunkt einer jeden datenschutzrechtlichen Betrachtung ist das so genannte „Verbotsprinzip mit Erlaubnisvorbehalt“: Demgemäß ist jede Verarbeitung personenbezogener Daten grundsätzlich untersagt – es sei denn, sie ist durch eine Rechtsgrundlage gedeckt. Hierbei kommen die datenschutzrechtliche Einwilligung und die gesetzlichen Erlaubnistatbestände in Betracht.[36] Beide stehen grundsätzlich gleichrangig nebeneinander.[37] Basierend auf der Forschungsfreiheit nach Art. 13 GRCh räumt die DS-GVO der Forschung für die Verarbeitung sensitiver Daten eine Privilegierung ein und somit eine Ausnahme vom Verbotsprinzip.[38] Für die Verarbeitung von Gesundheitsdaten ist somit zum einen die Einwilligung in Art. 9 Abs. 2 lit. a DS-GVO einschlägig. Zum anderen sieht die DS-GVO eine weitere Ausnahme vom Verbot der Verarbeitung für wissenschaftliche Zwecke in Art. 9 Abs. 2 lit. j vor. Außerdem kann bei der Verarbeitung von Gesundheitsdaten für Forschungszwecke auf Art. 9 Abs. 2 lit. h oder i zurückgegriffen werden. Dabei gilt die Privilegierung im Rahmen der Verordnung nur für die unabhängige, nicht kommerziell ausgerichtete Forschung.[39]

II. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Der datenschutzrechtliche Transparenzgrundsatz folgt aus der Erkenntnis, dass die betroffene Person nicht bloßes „Objekt“ einer Datenverarbeitung, sondern selbstbestimmtes Subjekt ist. Dies geht einher mit den verfassungsrechtlichen Anforderungen, die aus dem Grundrecht auf informationelle Selbstbestimmung folgen. Aus dem Transparenzgrundsatz folgt deshalb, dass der betroffenen Person alle Informationen zur Verfügung zu stellen sind, die für eine Einschätzung und Beurteilung der konkreten Verarbeitung ihrer personenbezogenen Daten erforderlich sind.[40] Der Transparenzgrundsatz verlangt von der verantwortlichen Stelle zum einen die transparente Ausgestaltung einer Einwilligungserklärung und zum anderen den transparenten Umgang mit personenbezogenen Daten.[41] Infolgedessen muss die betroffene Person zum Zeitpunkt der Datenerhebung über die konkrete Datenverarbeitung informiert werden. Zu den in der Datenschutzerklärung gem. Art. 13 f. DS-GVO notwendigen Angaben gehören die folgenden:

- Rechtsgrundlage der Datenverarbeitung: Tatbestände aus der DS-GVO bzw. aus dem nationalen Recht

[36] *Frenzel,* in: Paal/Pauly, DS-GVO BDSG, Art. 6 DS-GVO, Rn. 1.
[37] *Frenzel,* in: Paal/Pauly, DS-GVO BDSG, Art. 6 DS-GVO, Rn. 1.
[38] *Weichert*, in: Kühling/Buchner, DS-GVO BDSG, Art. 9 DS-GVO, Rn. 126.
[39] *Weichert*, in: Kühling/Buchner, DS-GVO BDSG, Art. 9 DS-GVO, Rn. 129, 130.
[40] *Schantz,* in: BeckOK-Datenschutzrecht, Art. 5 Rn. 11.
[41] *Heberlein,* in: Ehmann/Selmayr, Art. 5 DS-GVO, Rn. 11.

- Art, Umfang und Dauer der Datenverarbeitung: Welche Daten werden auf welche Weise durch welche Stelle für wie lange verarbeitet? Finden Datenübermittlungen an Dritte statt? Existiert ein fester Löschungszeitpunkt bzw. gibt es Anhaltspunkte zur Bestimmung der Speicherdauer?
- Zweck der Datenverarbeitung: Was wird mit der Datenverarbeitung bezweckt? Ist die Datenverarbeitung zur Erreichung dieses Zwecks tatsächlich erforderlich? Wird der benannte Zweck eingehalten bzw. findet eine Durchbrechung der Zweckbindung statt?
- Betroffenenrechte: Für jede Datenverarbeitung sind Informationen zu erteilen, welche jeweiligen Rechte den betroffenen Personen zur Verfügung stehen. Für den Fall der datenschutzrechtlichen Einwilligung ist auf die Möglichkeit des Widerrufs hinzuweisen.
- Kontaktdaten des Verantwortlichen: Nennung des Ansprechpartners für Datenschutzfragen, ggf. Kontakt des Datenschutzbeauftragten.
- Datenübermittlung in das Nicht-EU-Ausland: Bestehen gültige Datenschutzabkommen bzw. werden anderweitige Garantien vorgesehen, um einen angemessenen, dem europäischen Niveau entsprechenden Maßstab auch im Ausland zu gewährleisten?

III. Zweckbindung

Ein weiteres datenschutzrechtliches Verarbeitungsprinzip stellt der Zweckbindungsgrundsatz dar, der insbesondere eine Datenverarbeitung auf Vorrat verhindern soll.[42] So können personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer Weise verarbeitet werden, die mit diesen Zwecken unvereinbar ist, Art. 5 Abs. 1 lit. b DS-GVO. Der Art. 5 Abs. 1 lit. b DS-GVO stellt eine der elementarsten Privilegierungen der Forschung innerhalb der DS-GVO dar und normiert eine Fiktion der Vereinbarkeit mit den ursprünglichen Zwecken für wissenschaftliche Forschungszwecke.[43] Dir Vorschrift bestimmt, dass eine Weiterverarbeitung für wissenschaftliche Forschungszwecke nicht als unvereinbar mit den ursprünglichen Zwecken gilt. Insoweit verweist die Vorschrift auf Art. 89 DS-GVO. Eine Weiterverarbeitung muss dabei den geeigneten Garantien des Art. 89 Abs. 1 DS-GVO unterliegen.

Ein zentrales Anwendungsbeispiel für die zweckändernde Weiterverarbeitung im Kontext der Forschung von NFDI4Health ist das Record Linkage. Werden personenbezogene Daten zum Zweck des Record Linkage aus ihrem ursprünglichen Verarbeitungskontext herausgelöst, handelt es sich um eine zweckändernde Weiterverarbeitung, die den Datenschutzgrundsätzen entsprechend zulässig ist.

[42] *Heberlein,* in: Ehmann/Selmayr, DS-GVO, Art. 5, Rn. 25.
[43] *Herbst*, in: Kühling/Buchner, DS-GVO BDSG, Art. 5 DS-GVO, Rn. 50.

IV. Datenminimierung

Der Grundsatz der Datenminimierung bestimmt, dass sich die Datenerhebung auf das für die Verarbeitung erforderliche Maß beschränken sollte. Dies ist dann der Fall, wenn die Aufgabe des Verantwortlichen ohne die Datenverarbeitung nicht, nicht rechtzeitig, nicht vollständig oder nur mit einem unverhältnismäßigen Aufwand erfüllt werden könnte.[44] Entscheidende Frage ist somit – und dies gilt auch im Kontext der wissenschaftlichen Forschung – ob im Einzelfall eine ebenso effektive Alternative zur Datenverarbeitung mit geringerer Eingriffstiefe vorhanden ist.

Nach Art. 89 Abs. 1 S. 1 DS-GVO gilt, dass auch die Datenverarbeitung zu Forschungszwecken geeigneten Garantien für die Datenschutzrechte und -freiheiten unterliegen muss. Mit diesen Garantien soll sichergestellt werden, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Genannt wird in dem Zusammenhang auch die Pseudonymisierung.[45] Folglich findet sich der Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. b DS-GVO in Art. 89 Abs. 1 S. 2-4 DS-GVO als „geeignete Garantie" für die Verarbeitung zu wissenschaftlichen Forschungszwecken wieder.

V. Speicherbegrenzung

Ein ähnliches Ziel wie die Datenminimierung verfolgt der Grundsatz der Speicherbegrenzung, der jedoch weniger auf die Datenerhebung an sich, sondern im Kern auf den Umgang mit einmal erhobenen personenbezogenen Daten abstellt. So müssen personenbezogene Daten grundsätzlich in einer Form gespeichert werden, die eine Identifizierung der betroffenen Person nur so lange ermöglicht, wie dies zur Erreichung der Verarbeitungszwecke erforderlich ist, Art. 5 Abs. 1 lit. e DS-GVO. Eine Ausnahme vom Grundsatz der Speicherbegrenzung räumt die Vorschrift der wissenschaftlichen Forschung ein.[46] Personenbezogene Daten dürfen demnach, sofern sie ausschließlich für wissenschaftliche Forschungszwecke verarbeitet werden, länger gespeichert werden, soweit geeigneten Garantien gem. Art. 89 Abs. 1 DS-GVO getroffen werden.

VI. Datensicherheit

Der Grundsatz der Datensicherheit ist in Art. 5 Abs. 1 lit. f DS-GVO geregelt. Demgemäß müssen personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen so verarbeitet werden, dass eine angemessene technische Sicherheit (Datensicherheit) der personenbezogenen Daten gewährleistet ist. Hierzu gehört im Sinne der klassischen Ziele der IT-Sicherheit der Schutz vor unbefugter

[44] *Schantz*, in: BeckOK-Datenschutzrecht, Art. 5 DS-GVO, Rn. 25.
[45] *Weichert*, ZD 2020, 18, 22.
[46] *Herbst*, in: Kühling/Buchner, DS-GVO, Art. 5, Rn. 69.

oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Beschädigung.[47] Konkretisiert wird der Grundsatz der Datensicherheit insbesondere durch die Regelung in Art. 32 DS-GVO.

D. Übersicht über die rechtlichen Rahmenbedingungen der Datenverarbeitung zu Forschungszwecken

Das rechtliche Datenschutzregime zur Durchführung von wissenschaftlicher Forschung ist vielschichtig und knüpft an allgemeine sowie bereichsspezifische Regelungen an, die sich über verschiedene Regulierungsebenen zu einem hochkomplexen juristischen Gefüge verbinden. Hieraus ergeben sich erhebliche Herausforderungen in der Handhabung der Vorschriften zum Forschungsdatenschutz. Teils ist daher auch von einem „Flickenteppich" an datenschutzrechtlichen Regelungen für die Forschung die Rede.[48] Generell können zur Legitimation der Datenverarbeitung zu Forschungszwecken entweder die datenschutzrechtliche Einwilligung der betroffenen Person oder ein gesetzlicher Erlaubnistatbestand herangezogen werden. Je nach Verarbeitungssituation und Datenkategorie sind unterschiedliche Rechtsgrundlagen relevant, die im Folgenden anhand der datenschutzrechtlichen Legitimationsinstrumente dargestellt werden.

I. Datenschutzrechtliche Einwilligung

Zentrales Instrument zur Legitimation einer Verarbeitung von personenbezogenen Daten zu Forschungszwecken ist die datenschutzrechtliche Einwilligung der betroffenen Person.

Die Wirksamkeitsvoraussetzungen zur Erteilung der datenschutzrechtlichen Einwilligung sind in Art. 4 Nr. 11 DS-GVO legaldefiniert und beschreiben gleichzeitig die rechtliche Natur der Einwilligung: Diese ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.[49] Die tatbestandlichen Voraussetzungen („Bedingungen") für eine rechtswirksame Einwilligung sind in Art. 7 DS-GVO aufgelistet. Daneben stehen Art. 5 Abs. 1 lit. b und Art. 6 Abs. 1 lit. a DS-GVO für die Bestimmtheit der Einwilligung und Art. 8 für die Einwilligungsfähigkeit bei Minderjährigen. Für die Konkretisierung und Zusammenschau der zuvor genannten Vorschriften sind zudem die Erwägungsgründe 32 f. und 42 f. der DS-GVO zu berücksichtigen.[50]

---

[47] *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch, 50.1, Rn. 6 ff; *Schantz,* in: BeckOK-Datenschutzrecht, Art. 5 DS-GVO, Rn. 35 f.
[48] *Hänold*, ZD-Aktuell 2020, 07046.
[49] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO, Art. 4 Nr. 11, Rn. 1.
[50] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO, Art. 4 Nr. 11, Rn. 1.

1. Einwilligung als Erlaubnistatbestand

Die grundsätzliche Möglichkeit zur Einholung der Einwilligung als Legitimation einer Verarbeitung von personenbezogenen Daten ergibt sich allgemein aus Art. 6 Abs. 1 lit. a DS-GVO und für besondere Kategorien personenbezogener Daten aus Art. 9 Abs. 2 lit. a DS-GVO. Für die Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO gelten besondere Voraussetzungen. So muss sich die zu erteilende Einwilligung ausdrücklich auf die Verarbeitung sensitiver Daten beziehen.[51]

2. Freiwilligkeit

Eine grundlegende Voraussetzung der Einwilligung ist deren Freiwilligkeit gem. Art. 4 Nr. 11 DS-GVO. Für die Bestimmung der Freiwilligkeit bzw. Unfreiwilligkeit stellt die DS-GVO auf ein mögliches Ungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen ab.[52] Demnach ergeben sich in der datenschutzrechtlichen Praxis mit Blick auf die Freiwilligkeit der Einwilligung regelmäßig Probleme. So ist die Einwilligungserklärung der betroffenen Person nicht mehr als freiwillig anzusehen, wenn sie keine wirkliche oder freie Wahl hat bzw. nicht in der Lage ist, ihre Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden. Deshalb darf die Erteilung einer Einwilligung auch nicht als Bedingung für eine Gegenleistung verwendet werden (sog. „Koppelungsverbot“).[53] Von der Einholung einer Einwilligung sollte abgesehen werden, wenn die Datenverarbeitung bereits auf eine gesetzliche Erlaubnisgrundlage gestützt werden kann.

3. Bestimmtheit

Die Einwilligung muss für einen oder mehrere bestimmte Zwecke erteilt werden. Grundsätzlich muss die Zweckbestimmung so präzise wie möglich erfolgen.[54] Eine Einwilligungsklausel, die sich nicht auf bestimmte Datenverarbeitungen beschränkt und pauschal eingeholt wird, ist stets unwirksam.[55] Denn personenbezogene Daten dürfen gem. Art. 5 Abs. 1 lit. b DS-GVO nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Der Zweckbindungsgrundsatz erstreckt sich in diesem Rahmen auch auf die Einwilligung.[56]

---

[51] *Albers/Veit,* in: BeckOK-Datenschutzrecht, Art. 9 DS-GVO, Rn. 60.
[52] *Ernst,* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO, Rn. 71.
[53] *Buchner*, in: Kühling/Buchner, DS-GVO, Art. 4 Nr. 11, Rn. 6.
[54] *BfDI*, 29. Tätigkeitsbericht 2020, 40.
[55] *Ernst,* in: Paal/Pauly, DS-BVO BDSG, Art. 4 DS-GVO, Rn. 78.
[56] *Buchner*, in: Kühling/Buchner, DS-GVO, Art. 4 Nr. 11, Rn. 7.

Für den Fall der wissenschaftlichen Forschung kann auf die Besonderheit der erweiterten Einwilligung, auch bekannt als „Broad Consent", zurückgegriffen werden.[57] So kann oftmals der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Der Erwägungsgrund 33 der Verordnung sieht daher vor, dass betroffene Personen ihre Einwilligung lediglich für bestimmte Bereiche wissenschaftlicher Forschung erteilen, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Dabei ist zu beachten, dass die betroffenen Personen die Gelegenheit erhalten sollten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maß zu erteilen.[58] Allerdings unterliegt der flexible Ansatz des Erwägungsgrundes 33 unter Berücksichtigung der strengen Auflagen des Art. 9 DS-GVO einer strengeren Auslegung für die Verarbeitung besonderer Kategorien von Daten.[59] Der Broad Consent soll damit nicht eine Möglichkeit darstellen, den Zweckbindungsgrundsatz zu umgehen, denn die erweiterte Einwilligung soll weiterhin nur als Ausnahme zur Anwendung erlangen, wenn eine genaue Bezeichnung des Zwecks nicht möglich ist.[60] Der Verantwortliche muss für den Fall des Broad Consent nach anderen Wegen suchen, um sicherzustellen, dass dem Wesensgehalt der Einwilligung Rechnung getragen wird, beispielsweise durch Einwilligung in einen allgemeinen, aber so gut wie möglich beschriebenen, Forschungsbereich oder für eine bestimmte Phase eines Forschungsprojekts, welche von Anfang an bekannt und bestimmbar ist.[61] In diesem Rahmen kann die verantwortliche Stelle ebenso mehr Garantien, wie die Datenminimierung, Anonymisierung und Datensicherheit gewährleisten.[62] Die Medizininformatik-Initiative (MII) des BMBF hat für die Verarbeitung von Gesundheitsdaten zu Forschungszwecken Mustertexte bestehend aus einer Patienteninformation und einer Einwilligungserklärung sowie einer Handreichung speziell für den Broad Consent erarbeitet.[63] Die Einwilligungsdokumente wurden von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder beratend begleitet und nach einem intensiven Abstimmungsprozess mit Beschluss vom 15. April 2020 akzeptiert. Die Einwilligungsdokumente ermöglichen eine standortübergreifende kontrollierte Nutzung und Bereitstellung von Patientendaten zu medizinischen Forschungszwecken.[64]

[57] *Cepic*, ZD-Aktuell 2021, 05214.
[58] *Weichert,* in: Kühling/Buchner, DS-GVO BDSG, Art. 9 DS-GVO, Rn. 51a.
[59] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung, 34.
[60] *BfDI*, 29. Tätigkeitsbericht 2020, 40.
[61] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung, 34 f.
[62] *Artikel-29-Datenschutzgruppe,* Leitlinien in Bezug auf die Einwilligung, 35.
[63] AG Consent des Nationalen Steuerungsgremiums der MII des BMBF, Handreichung, S.2.
[64] AG Consent des Nationalen Steuerungsgremiums der MII des BMBF, Handreichung, S.2.

4. Informiertheit

Die informierte Einwilligung oder auch Einwilligung nach erfolgter Aufklärung ist neben der Freiwilligkeit und Bestimmtheit ein weiterer Grundsatz, der im Rahmen einer wirksamen Einwilligungserteilung Beachtung finden muss.[65] Eine Einwilligung ist in diesem Rahmen nur wirksam, wenn sie in informierter Weise erfolgt.[66] Indem die Einwilligung der informierten Willenserklärung der betroffenen Person im Einzelfall bedarf, sollte diese sich der Umstände der Rechtsgrundlage der Datenverarbeitung, der Identität des Verantwortlichen und der Zweckbestimmung der verarbeiteten personenbezogenen Daten bewusst sein und die Tragweite der Einwilligung eindeutig und klar erkennen.[67] Für die Fälle des Broad Consents in der Forschung kann die Informiertheit in der Praxis besondere Herausforderungen mit sich bringen, die beispielsweise darin liegen, eine möglichst allgemeinverständliche Beschreibung von Forschungsvorhaben und Zwecken vorzunehmen.[68]

5. Weitere Bedingungen der wirksamen Einwilligungserteilung

Art. 7 Abs. 1 DS-GVO statuiert weitere formale Wirksamkeitsvoraussetzungen hinsichtlich der Form, Transparenz, dem Zeitpunkt und der betroffenen Person. So muss der für die Verarbeitung Verantwortliche nachweisen können, dass die betreffende Person ihre Einwilligung erteilt hat. Die DS-GVO stellt zwar keine formalen Anforderungen an die Zustimmung zur Datenverarbeitung, sodass diese sowohl mündlich als auch schriftlich und elektronisch erteilt werden kann, jedoch ist zur besseren Nachweisbarkeit der erteilten Einwilligung in der Praxis die Textform zu empfehlen. Eine schriftliche Einwilligungserklärung sollte in leichter und verständlicher Form und Sprache ausgestaltet sein.

6. Widerrufbarkeit

Eine Besonderheit der datenschutzrechtlichen Einwilligung ist darin zu sehen, dass die betroffene Person gem. Art. 7 Abs. 3 DS-GVO das Recht hat, die Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Der Verantwortliche muss bei Erteilung der Einwilligung über die Möglichkeit des Widerrufs informieren. Das Widerrufsrecht ist eines der elementaren Rechte, welches betroffenen Personen im Rahmen der DS-GVO gewährt wird. Es soll sicherstellen, dass die betroffene Person im Sinne der informationellen Selbstbestimmung in der Lage ist, ihre Entscheidung zu revidieren bzw. abzuändern.[69] Durch

[65] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, Art. 4 Nr. 11 DS-GVO, Rn. 8.
[66] *Weichert*, Datenschutzrechtliche Bestimmungen medizinischer Forschung, 95.
[67] *Cepic*, ZD-Aktuell 2021, 05214.
[68] *Golla*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 23, Rn. 23.
[69] *Buchner*, in: Kühling/Buchner, DS-GVO BDSG, Art. 7 DS-GVO, Rn. 34.

den Widerruf der erteilten Einwilligung wird jedoch die Rechtmäßigkeit der bis dahin erfolgten Datenverarbeitung nicht berührt. Dabei gilt, dass der Widerruf genauso einfach sein muss wie das Erteilen der Einwilligung. Die elektronisch erteilte Einwilligung setzt mithin die Möglichkeit zum elektronischen Widerruf voraus. Aufgrund dieser jederzeitigen Widerrufbarkeit sollten Verantwortliche grundsätzlich sicherstellen, dass eine Beendigung der Datenverarbeitung nach Widerruf noch möglich ist. Dies setzt entsprechende Managementprozesse zur Datenverarbeitung voraus. Das Widerrufsrecht bleibt auch für den Broad Consent trotz der weiten Zweckfestlegung bestehen.[70]

7. Verfallsdatum

Die DS-GVO sieht grundsätzlich keine zeitliche Begrenzung bei einer einmal erteilten Einwilligung vor. Es gilt, dass eine Einwilligung grundsätzlich solange gilt, bis sie widerrufen wird. Ein automatischer Zeitablauf für eine Einwilligung ist somit in der Verordnung nicht vorgesehen.[71] Allerdings empfiehlt die Artikel-29-Datenschutzgruppe (WP 29), die Einwilligung in angemessenen Zeitabständen zu erneuern.[72] Hierzu wird angeführt, dass bei einer Erneuerung der Einwilligung die betroffene Person über die Datenverarbeitung und Rechtsausübung informiert bleibt.[73]

8. Bereichsspezifische Anforderungen an die Einwilligung in der Forschung mit Sozialdaten

Für die Verarbeitung von Sozialdaten, die ebenfalls personenbezogene Daten sind (§ 67 Abs. 2 S. 1 SGB X), gelten gem. § 67b SGB X im Forschungskontext bereichsspezifische Besonderheiten. Dies folgt aus der Vorschrift in § 35 Abs. 2 S. 1 SGB I, wonach die sozialrechtlichen Datenschutzvorschriften grds. abschließend gelten und insoweit Vorrang vor den allgemeinen datenschutzrechtlichen Anforderungen aus der DS-GVO haben. Auch hier ist jedoch die Möglichkeit eines *Broad Consent* zur Einwilligungserteilung vorgesehen, indem in § 67b Abs. 3 SGB X festgestellt wird, dass die Einwilligung zur Verarbeitung personenbezogener Daten zu Forschungszwecken für ein bestimmtes Vorhaben oder für bestimmte Bereiche der wissenschaftlichen Forschung erteilt werden kann. Eine besondere Vorschrift im Sozialrecht zur Übermittlung von Sozialdaten für die Forschung und Planung enthält mit Blick auf die Einwilligung der § 75 SGB X. Die Vorschrift ist insoweit hervorzuheben, als dass sie gesetzlich festgelegte tatbestandliche Erfordernisse mit der datenschutzrechtlichen Einwilligung kombiniert.[74] Dabei gilt, dass eine Übermittlung

[70] *Golla*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 23, Rn. 22; *Herbst*, DuD 2016, 371, 373 f.
[71] *Heckmann/Paschke*, in: Ehmann/Selmayr, DS-GVO, Art. 7, Rn. 43.
[72] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung, 25.
[73] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung, 25.
[74] *Westphal*, in: BeckOK-Sozialrecht, § 75 SGB X, Rn. 3 ff.

ohne Einwilligung der betroffenen Person nicht zulässig ist, soweit es zumutbar ist, ihre Einwilligung einzuholen.

9. Datenschutzrechtliche Einwilligung und Schweigepflichtentbindung

Gem. Art. 9 Abs. 3 DS-GVO bleibt das nationale Recht zu Berufsgeheimnissen neben den datenschutzrechtlichen Vorgaben bestehen. Für die (Weiter-)Verarbeitung von Gesundheitsdaten, die eine Offenbarung von Patientengeheimnissen erforderlich machen, muss deshalb die Unterscheidung der datenschutzrechtlichen Einwilligung und der Entbindung von der beruflichen Schweigepflicht beachtet werden.[75] Die berufliche Schweigepflicht ergibt sich in Deutschland aus § 203 StGB und gilt für eine Vielzahl von Berufen. Für die medizinische Forschung sind insbesondere die in der Norm aufgezählten Berufsausübenden im Gesundheitsbereich signifikant.[76]

Durch die Erklärung einer Schweigepflichtentbindung kann die betroffene Person die berufliche Schweigepflicht aufheben[77] und die Datenverarbeitung bzw. Weitergabe legitimieren und sodann z.B. für Forschungszwecke nutzbar zu machen. Neben der datenschutzrechtlichen Einwilligung bedarf es demnach einer zusätzlichen Offenbarungsbefugnis.[78] Letztgenannte muss ebenfalls auf freier Willensbildung und Entscheidung ausdrücklich oder konkludent durch den Patienten erfolgen.[79] Dazu muss diese hinreichend bestimmt sein. Der Zweck der Datenweitergabe spielt hier eine zentrale Rolle. Das Einholen einer pauschalen Einwilligung bei Abschluss eines Behandlungsvertrages für alle Fälle einer Datenweitergabe ist nicht zulässig.[80] Auch die Einwilligung zur Entbindung von einer beruflichen Schweigepflicht kann jederzeit mit Wirkung für die Zukunft widerrufen werden.[81] Trotz Übereinstimmungen stellen sich die Anforderungen einer datenschutzrechtlichen Einwilligung in einigen Aspekten strenger als die einer Schweigepflichtentbindung dar.[82] Der Datenschutz und die ärztliche Schweigepflicht sind rechtlich unabhängig voneinander zu betrachten, sodass die datenschutzrechtliche Einwilligung und die Entbindung von der ärztlichen Schweigepflicht nicht gleichzusetzen sind, auch wenn sie gemeinsam erklärt werden können. Dabei muss allerdings beachtet werden, dass eine Kenntlichmachung der von der Einwilligung erfassten Daten, die zugleich einem Berufsgeheimnis unterliegen, erfolgt. Hierbei müssen die Anforderungen für die Datenverarbeitung und gleichzeitig für die Schweigepflichtentbindung erfüllt werden.[83]

---

[75] *Weichert,* in: Kühling/Buchner, DS-GVO BDSG, Art. 9 Rn. 49, 50.
[76] *Weichert,* Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, S. 74.
[77] *Weichert*, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, S. 76.
[78] *Weichert,* in: Kühling/Buchner, DS-GVO BDSG, Art. 9 Rn. 146-148.
[79] Deutsches Ärzteblatt, DOI:10.3238./aertzebl.2021.ds02, S.3.
[80] Deutsches Ärzteblatt, DOI:10.3238./aertzebl.2021.ds02, S.3.
[81] OLG München, Urteil vom 16.05.2013 – 1 U 4156/12.
[82] *Weichert*, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, S. 78.
[83] *Weichert,* in: Kühling/Buchner, DS-GVO BDSG, Art. 9 Rn. 49.

Aus den vorangehenden Ausführungen folgt ebenfalls, dass bei der Verarbeitung von Daten durch Fachpersonal mit Berufsgeheimnissen das sogenannte „Zwei-Schranken-Prinzip“ zu beachten ist.[84] Bei Datenverarbeitungen, die grundsätzlich den datenschutzrechtlichen Vorgaben unterliegen und zudem von einem Berufsgeheimnis umfasst sind, muss somit eine zweistufige Prüfung erfolgen, da beide Rechtsgebiete unabhängig voneinander bestehen bleiben und einander bedingen.[85] Beispielsweise würde eine Datenverarbeitung bzw. -übermittlung, die datenschutzrechtlich durch einen der Tatbestände des Art. 9 Abs. 2 DS-GVO legitimiert wäre, dabei aber gleichzeitig gegen ein Berufsgeheimnis verstößt, insgesamt als unzulässig eingestuft werden.[86]

II. Gesetzliche Erlaubnistatbestände

Neben der datenschutzrechtlichen Einwilligung kommen gesetzliche Erlaubnistatbestände für die personenbezogene Datenverarbeitung zu Forschungszwecken in Betracht. Zu unterscheiden ist dabei zwischen den allgemeinen und den bereichsspezifischen Regelungen.

Das im Rahmen der allgemeinen Datenverarbeitungsgrundsätze bereits vorgestellte und in Art. 89 DS-GVO verankerte Forschungsprivileg räumt der zu Forschungszwecken erfolgenden Datenverarbeitung zwar verschiedene rechtliche Begünstigungen ein – Art. 89 DS-GVO enthält selbst jedoch keine Rechtsgrundlage zur Verarbeitung von personenbezogenen Daten.[87]

Bei der Bestimmung der geeigneten Rechtsgrundlage ist überdies nicht nur zwischen allgemeinen und bereichsspezifischen Regelungen, sondern ebenso zwischen den unterschiedlichen Datenkategorien zu unterscheiden: „allgemeine“ personenbezogene Daten (Art. 6 DS-GVO) und sog. besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO).

Im Folgenden werden der allgemeine gesetzliche Erlaubnistatbestand des § 27 BDSG sowie der bereichsspezifische Erlaubnistatbestand des § 75 SGB X und die bereichsspezifischen Erlaubnistatbestände für die Krebsregister mit ihren jeweiligen Besonderheiten vorgestellt.

Eine systematische Übersicht über den gesamten Regelungszusammenhang für die wissenschaftliche und gesundheitsbezogene Forschung im Rahmen von NFDI4Health findet sich in der nachfolgenden tabellarischen Legal Map.

[84] *March et al.*, Gesundheitswesen 2019; 81, S. 636 und *Weichert,* in: Kühling/Buchner, DS-GVO BDSG, Art. 9 Rn. 138.
[85] *Weichert,* Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, S. 78.
[86] *Weichert,* in: Kühling/Buchner, DS-GVO BDSG, Art. 9 Rn. 146.
[87] *Raum,* in: Ehmann/Selmayr, DS-GVO, Art. 89, Rn. 1.

1. Allgemeiner Erlaubnistatbestand: § 27 BDSG

Als allgemeiner gesetzlicher Erlaubnistatbestand für die Datenverarbeitung im Kontext der wissenschaftlichen Forschung zu berücksichtigen ist § 27 BDSG, dem eine Auffangfunktion gegenüber bereichsspezifischen Datenschutzregelungen zukommt.[88] Die bereichsspezifischen Regelungen zur Datenverarbeitung für Forschungszwecke genießen somit Vorrang zu § 27 BDSG. Dabei sind die einschlägigen Normen aus den Landesdatenschutzgesetzen, Sozialgesetzbüchern und weiteren medizinrechtlichen Gesetzen zu beachten.[89] Bei der Anwendbarkeit der Gesetze muss zudem eine Unterscheidung der Verantwortlichen einer Datenverarbeitung im Hinblick auf ihre Trägerschaft erfolgen. Hierbei ist zwischen öffentlichen Stellen (z.B. Universitäten und Hochschulen) und privaten Einrichtungen wie Unternehmen und Vereinen zu differenzieren.

Gem. § 27 Abs. 1 BDSG ist die Verarbeitung besonderer Datenkategorien auch ohne Einwilligung für wissenschaftliche Forschungszwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.

Strittig ist, wann von einem erheblichen Überwiegen der Interessen auszugehen ist.[90] Vorzunehmen ist hierzu eine Berücksichtigung, Gewichtung und Abwägung der grundrechtlichen Positionen.[91] In jedem Falle einzubeziehen ist das wissenschaftliche Interesse, das im Lichte der verfassungsrechtlich gewährleisteten Wissenschaftsfreiheit zu berücksichtigen ist.[92] Für die Durchführung eines Forschungsvorhabens dürften regelmäßig Allgemeinwohlinteressen sprechen. Das führt auch dazu, dass ein Überwiegen des Forschungsinteresses dann zu bejahen sein wird, wenn ein Forschungsvorhaben erhebliche Verbesserungen für die Gesundheit oder die soziale Sicherheit der Bevölkerung mit sich bringt.[93] Wie für die allgemeine datenschutzrechtliche Interessenabwägung auch kann bestimmten thematischen Vorhaben jedoch nicht im Sinne eines Automatismus ein höherwertiges Interesse eingeräumt werden – insoweit wird zunächst nicht zwischen unterschiedlichen Forschungsbereichen unterschieden. Jede wissenschaftliche Forschung sollte aber durchgängig wissenschaftlichen Ansprüchen genügen, um in den Genuss einer Privilegierung im Sinne der Interessenabwägung zu gelangen.[94]

[88] *Klar*, in: Kühling/Buchner, DS-GVO BDSG, § 1 BDSG, Rn. 14.
[89] *Buchner/Tinnefeld*, in: Kühling/Buchner, DS-GVO BDSG, § 27 BDSG, Rn. 26.
[90] *Louven*, in: Taeger/Gabel, DS-GVO BDSG, § 27, Rn. 9.
[91] *Louven*, in: Taeger/Gabel, DS-GVO BDSG, § 27, Rn. 9.
[92] *Buchner/Tinnefeld*, in: Kühling/Buchner, DS-GVO BDSG, § 27 BDSG, Rn. 12.
[93] *Krohm,* in: Gola/Heckmann, BDSG, § 27, Rn. 24.
[94] Vgl. *Buchner/Tinnefeld*, in: Kühling/Buchner, DS-GVO BDSG, § 27 BDSG, Rn. 12.

Die Interessenabwägung gem. § 27 Abs. 1 BDSG und ihr Ergebnis sind zu dokumentieren, da die forschende Stelle für das Überwiegen der Interessen nachweispflichtig ist.[95] Hierbei sind die zuvor genannten Kriterien zu berücksichtigen.[96] In der Praxis wird regelmäßig deutlich, dass die Durchführung der geforderten Interessenabwägung durch verantwortliche Forschungseinrichtungen erhebliche Schwierigkeiten mit sich bringt.[97] Daher ist es sinnvoll, den Datenschutzbeauftragten hinzuzuziehen und in unklaren Fällen bzw. um eine rechtssichere Datenverarbeitung zu gewährleisten, die Aufsichtsbehörde um Stellungnahme zu bitten. Der damit verbundene organisatorische Aufwand wiederum führt jedoch letztlich zur Beeinträchtigung von Forschungsvorhaben.[98]

2. Bereichsspezifischer Erlaubnistatbestand: § 75 SGB X

Bereits im Rahmen der bereichsspezifischen Anforderungen der Einwilligung in der Forschung wurde die Vorschrift des § 75 SGB X als besondere Regelung aus dem Sozialdatenschutz skizziert, da sie gesetzliche Anforderungen mit der Einwilligung verknüpft. Die Übermittlung von Sozialdaten ist in diesem Rahmen zulässig, soweit sie u.a. erforderlich ist für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich und schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse der betroffenen Person erheblich überwiegt. Dabei gilt aber, dass eine Übermittlung ohne Einwilligung der betroffenen Person nicht zulässig ist, soweit es zumutbar ist, ihre Einwilligung einzuholen. Lediglich Angaben über den Namen und Vornamen, die Anschrift, die Telefonnummer sowie die für die Einleitung eines Forschungsvorhabens zwingend erforderlichen Strukturmerkmale der betroffenen Person können für Befragungen auch ohne Einwilligung übermittelt werden. Die Ausnahmen vom Einwilligungserfordernis werden für diese Forschungsklausel teilweise eng verstanden. Argumentiert wird, dass als Grenze der Zumutbarkeit lediglich ein unverhältnismäßiger Aufwand im Einzelfall gelten kann und der Verzicht auf die Einwilligung der betroffenen Person deshalb lediglich auf absolute Ausnahmefälle beschränkt ist.[99] Dem kann jedoch nicht ohne Weiteres gefolgt werden, denn vielfach dürfte die Durchführung von Großforschungsvorhaben mit Krankenkassendaten mit einer zusätzlichen Einwilligung nicht zumutbar sein. Gerade für den Bereich der Forschungsdatenverarbeitung lässt sich die DS-GVO durchaus auch so verstehen, dass kein Primat der Einwilligung gilt.[100] Für die Datenverarbeitung nach § 75 SGB X ist weiterhin zu berücksichtigen, dass eine entsprechende Übermittlung von Sozialdaten nur zulässig ist, soweit grds.

[95] *Herbst,* in: Kasseler Kommentar zum Sozialversicherungsrecht, § 75 SGB X, Rn. 67.
[96] *Rat für Sozial- und WirtschaftsDaten*, Handreichung Datenschutz, 18.
[97] *Krohm*, in: Gola/Heckmann, BDSG, § 27, Rn. 28.
[98] Vgl. *Krohm*, in: Gola/Heckmann, BDSG, § 27, Rn. 27 f.
[99] *Herbst*, in: Kasseler Kommentar zum Sozialversicherungsrecht, § 75 SGB X, Rn. 69.
[100] *Buchner/Haber/Hahn/Kusch/Prasser/Sax/Schmidt*, DuD 2021, 806, 809.

die vorherige Genehmigung durch die oberste Bundes- oder Landesbehörde, die für den Bereich, aus dem die Daten herrühren, zuständig ist, vorliegt.

3. Bereichsspezifische Erlaubnistatbestände für die Krebsregister

Die Erhebung von Daten aus den Krebsregistern der Länder ist aufgrund der unterschiedlichen datenschutzrechtlichen Rahmenbedingungen der Länder mit ganz erheblichen Herausforderungen verbunden. Eine Übersicht der verschiedenen landesgesetzlichen Regelungen findet sich in der nachfolgenden Legal Map.

Mit Blick auf die Verwendung von Krebsregisterdaten zu Zwecken der wissenschaftlichen Forschung ergeben sich aber zumindest Erleichterungen durch das Gesetz zur Zusammenführung von Krebsregisterdaten vom 18. August 2021[101]. Das Zentrum für Krebsregisterdaten hat nach § 2 BKRG die Aufgaben der Zusammenführung und der Prüfung der von den Krebsregistern übermittelten Daten gem. § 6 Abs. 2 Nr. 1 BKRG sowie der Erstellung eines Datensatzes nach Maßgabe des § 6 Abs. 2 Nr. 2 BKRG und der Durchführung von Studien und Analysen nach Maßgabe des § 6 Abs. 2 Nr. 3 BKRG. Die Förderung der wissenschaftlichen Nutzung der beim Zentrum für Krebsregisterdaten vorliegenden Daten nach Maßgabe des § 8 BKRG sowie die Einrichtung einer zentralen Antrags- und Registerstelle nach Maßgabe des § 10 BKRG sind ebenfalls Aufgaben des Zentrums. Die Berechtigung zum Empfang der Daten aus den Landeskrebsregistern ergibt sich mit den gesetzlichen Änderungen aus § 5 Abs. 1 BKRG und zur Verwendung der erhaltenen Daten zur Prüfung auf Einheitlichkeit, Vollständigkeit und Vollzähligkeit sowie zur Erstellung eines bundesweit einheitlichen Datensatzes aus § 6 Abs. 1, Abs. 2 Nr. 1, Nr. 2 BKRG. Das Bundeskrebsregister übermittelt den Landeskrebsregistern die Ergebnisse seiner Prüfung auf Einheitlichkeit und Vollständigkeit gem. § 7 Abs. 1 BKRG. Daten können zu Forschungszwecken an Dritte gem. § 8 Abs. 1 BKRG übermittelt werden, soweit im entsprechenden Antrag nachvollziehbar dargelegt ist, dass der Umfang und die Struktur der beantragten Daten geeignet und erforderlich sind, um die zu untersuchenden Fragen zu beantworten und das im Antrag angegebene Vorhaben mit den beim Zentrum für Krebsregisterdaten vorliegenden Daten bearbeitet werden kann und eine länderübergreifende Auswertung erfordert. Allerdings unterliegt die Datenübermittlung und -bereitstellung diversen Anforderungen und Einschränkungen, u.a. der Antragstellung (Abs. 1), der Übermittlung der Daten in anonymisierter Form (Abs. 1) sowie einer Bewertung des Re-Identifizierungs-Risikos und des Treffens geeigneter Gegenmaßnahmen (Abs. 5). Abweichend von Abs. 1 kann bei Erforderlichkeit und entsprechender Begründung durch den Datenempfänger eine Bereitstellung pseudonymisierter Einzeldatensätze erfolgen (Abs.

[101] BGBl. 2021 I, 3890.

6). In diesem Rahmen gelten weitere besondere Anforderungen, um dem Persönlichkeitsschutz der betroffenen Personen gerecht zu werden: So dürfen die pseudonymisierten Datensätze nur Personen bereitgestellt werden, die einer Geheimhaltungspflicht gem. § 203 StGB unterliegen oder vor dem Zugang zur Geheimhaltung verpflichtet wurden (Abs. 7). Durch diese zusätzlichen Anforderungen werden die Möglichkeiten zur praxisgerechten Forschung mit Krebsregisterdaten erheblich erschwert oder sogar in vielen Fällen unmöglich gemacht. Eine Möglichkeit zur Überwindung dieser Limitationen könnte darin zu sehen sein, dass das Gesetz zur Zusammenführung von Krebsregisterdaten in § 10 BKRG bis zum 31.12.2024 den Auftrag zur Erarbeitung eines Konzepts zur Schaffung einer Plattform, die eine bundesweite anlassbezogene Datenzusammenführung und Analyse der Krebsregisterdaten aus den Ländern sowie eine Verknüpfung von Krebsregisterdaten mit anderen Daten ermöglicht und die klinisch-wissenschaftliche Auswertung der Krebsregisterdaten fördert, formuliert. Die Belange des Datenschutzes und der Informationssicherheit sind bei der Konzepterstellung entsprechend zu berücksichtigen.

4. Legal Map: Übersicht über Forschungstatbestände im Datenschutzrecht

Die nachfolgende Tabelle enthält eine Übersicht über die relevanten Rechtsvorschriften im Datenschutz für die Forschung und untergliedert sich in europäische Regelungen sowie in Bundes- und Landesgesetzgebung. Flankiert wird die Übersichtstabelle durch den Anhang zu diesem Deliverable, der die relevanten Forschungsvorschriften mit Datenschutzbezug im Volltext enthält.

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
Bundesdatenschutzgesetz (BDSG)		
BDSG	§ 1	Anwendungsbereich des Gesetzes
BDSG	§ 22	Verarbeitung besonderer Kategorien personenbezogener Daten
BDSG	§ 27	Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
BDSG	§ 50	Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken
Datenschutzrecht der Länder		
Baden-Württemberg (BW LDSG)	§ 13	Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
Bayern (BayDSG)	Art. 25	Verarbeitung zu Forschungszwecken

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
Berlin (BlnDSG)	§§ 17, 35	- Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken - Verarbeitung zu wissenschaftlichen, historischen, archivarischen und statistischen Zwecken
Brandenburg (BbgDSG)	§ 25	Datenverarbeitung für wissenschaftliche und historische Forschungszwecke
Bremen (BremDS-GVOAG)	§ 13	Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken
Hamburg (HmbDSG)	§ 11	Datenverarbeitung zum Zwecke wissenschaftlicher und historischer Forschung sowie Statistik
Hessen (HDSIG)	§§ 24, 45	- Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken - Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken, archivarischen oder statistischen Zwecken
Mecklenburg-Vorpommern (DSG M-V)	§ 9	Datenverarbeitung für wissenschaftliche oder historische Forschung
Niedersachsen (NDSG)	§ 13	Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken
Nordrhein-Westfalen (DSG NRW)	§ 17	Datenverarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken
Rheinland-Pfalz (LDSG RLP)	§§ 22, 31	- Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken - Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
Saarland (SDSG)	§ 23	Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken
Sachsen (SächsDSDG)	§ 12	Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken
Sachsen-Anhalt (DSAG LSA)	§ 27	Ausnahmen in Bezug auf die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken nach Artikel 89 der Verordnung (EU) 2016/679
Schleswig-Holstein (LDSG SH)	§§ 13, 26	- Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken - Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken
Thüringen (ThürDSG)	§ 28	Verarbeitung personenbezogener Daten durch Forschungseinrichtungen
Vertrag über die Arbeitsweise der Europäischen Union (AEUV)		
AEUV	Art. 179	Europäischer Raum der Forschung
EU Datenschutz-Grundverordnung (DS-GVO)		
DS-GVO	Art. 4 Nr. 1	Begriffsbestimmung "Personenbezogene Daten"
DS-GVO	Art. 4 Nr. 2	Begriffsbestimmung "Verarbeitung"
DS-GVO	Art. 5	Grundsätze für die Verarbeitung personenbezogener Daten
DS-GVO	Art. 6 Abs. 1 S. 1	Rechtmäßigkeit der Verarbeitung
DS-GVO	Art. 6 Abs. 1 S. 1 lit. a	Rechtmäßigkeit der Verarbeitung: Einwilligung
DS-GVO	Art. 6 Abs. 1 S. 1 lit. f	Rechtmäßigkeit der Verarbeitung: Interessenabwägung
DS-GVO	Art. 7	Bedingungen für die Einwilligung
DS-GVO	Art. 9 Abs. 1	Verarbeitung besonderer Kategorien personenbezogener Daten und Begriffsbestimmung

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
DS-GVO	Art. 9 Abs. 2 lit. a	Verarbeitung besonderer Kategorien personenbezogener Daten: Einwilligung
DS-GVO	Art. 9 Abs. 2 lit. g	Datenverarbeitung aus Gründen eines erheblichen öffentlichen Interesses (mitgliedstaatliche Öffnungsklausel)
DS-GVO	Art. 9 Abs. 2 lit. h	Individuelle Versorgung im Gesundheitsbereich
DS-GVO	Art. 9 Abs. 2 lit. i	Öffentliche Gesundheitsbelange
DS-GVO	Art. 9 Abs. 2 lit. j	Archivarische, wissenschaftliche und historische Forschungszwecke sowie statische Zwecke
DS-GVO	Art. 12	Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
DS-GVO	Art. 13	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
DS-GVO	Art. 14 Abs. 5	Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Ausnahme für Forschung)
DS-GVO	Art. 15	Auskunftsrecht der betroffenen Person
DS-GVO	Art. 16	Recht auf Berichtigung
DS-GVO	Art. 17 Abs. 3	Recht auf Löschung inkl. „Recht auf Vergessenwerden“ (Abs. 3 enthält Ausnahme für Forschung)
DS-GVO	Art. 21 Abs. 6	Widerspruchsrecht bei Datenverarbeitung zu Forschungszwecken
DS-GVO	Art. 85	Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit unter Einbeziehung wissenschaftlicher Zwecke
DS-GVO	Art. 89	Garantien und Ausnahmen in Bezug auf die Verarbeitung zu […] wissenschaftlichen […] Zwecken
EU-Grundrechtecharta (GRCh)		
GRCh	Art. 7	Achtung des Privat- und Familienlebens

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
GRCh	Art. 8	Schutz personenbezogener Daten
GRCh	Art. 13	Freiheit der Kunst und der Wissenschaft
Gesundheitsdienstgesetze der Länder (GDG)		
Baden-Württemberg	§ 18	Verarbeitung (auch zu Forschungszwecken)
Bayern	Keine Vorschrift zur forschungsspezifischen Datenverarbeitung	
Berlin	§ 5	Integrierte Gesundheitsberichterstattung
Brandenburg	Keine Vorschrift zur forschungsspezifischen Datenverarbeitung	
Bremen	§ 36	Datenverarbeitung für Forschungszwecke
Hamburg	§ 28	Forschung mit personenbezogenen Daten
Hessen	Keine Vorschrift zur forschungsspezifischen Datenverarbeitung	
Mecklenburg-Vorpommern	Keine Vorschrift zur forschungsbezogenen Datenverarbeitung	
Nordrhein-Westfalen	Keine Vorschrift zur forschungsbezogenen Datenverarbeitung	
Rheinland-Pfalz	§ 11	Datenschutz
Saarland	Keine Vorschrift zur forschungsbezogenen Datenverarbeitung	
Sachsen	Keine Vorschrift zur forschungsbezogenen Datenverarbeitung	
Sachsen-Anhalt	Keine Vorschrift zur forschungsbezogenen Datenverarbeitung	
Schleswig-Holstein	Kein Forschungsbezug, § 16 Abs. 1 S. 2 regelt die Einwilligung als Rechtsgrundlage zur Datenverarbeitung	Datenschutz
Thüringen	Keine Vorschrift zur forschungsbezogenen Datenverarbeitung	
Grundgesetz (GG)		
GG	Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1	Persönliche Freiheitsrechte: Allgemeines Persönlichkeitsrecht, Recht auf informationelle Selbstbestimmung, Computer-Grundrecht

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
GG	Art. 5 Abs. 3	Wissenschaftsfreiheit
Infektionsschutzgesetz (IfSG)		
IfSG	§ 14 Abs. 1	Elektronisches Melde- und Informationssystem
IfSG	§ 14 Abs. 4	Elektronisches Melde- und Informationssystem: automatisierte Überprüfung
Krankenhausgesetze der Länder (LKHG)		
Baden-Württemberg	LKHG gilt für Forschung nicht, vgl. § 43 Abs. 3; nur für krankenhausinterne Forschung, vgl. § 46 Abs. 1 Nr. 2a	Zulässigkeit der Übermittlung
Bayern	Art. 27 Abs. 1 S. 2, Abs. 5 schränken § 27 BDSG (Datenverarbeitung zu wissenschaftlichen Forschungszwecken) nicht ein	Datenschutz
Berlin	§ 25	Verarbeitung von genetischen Daten und Gesundheitsdaten zu wissenschaftlichen Forschungszwecken
Brandenburg	§ 31	Datenschutz bei Forschungsvorhaben
Bremen	§ 39 Abs. 2	Verarbeitung von Patientendaten zu Forschungszwecken
Hamburg	§ 12	Forschungsvorhaben und Sammlungen von Proben
Hessen	Keine Vorschrift zum forschungsbezogenen Datenschutz	
Mecklenburg-Vorpommern	§ 37	Datenverarbeitung für Forschungszwecke
Niedersachsen	Keine Vorschrift zum forschungsbezogenen Datenschutz	
Nordrhein-Westfalen	Nicht LKHG, aber § 6 Gesundheitsdatenschutzgesetz (GDSG) NRW	Datenverarbeitung für wissenschaftliche Zwecke
Rheinland-Pfalz	§ 37 Abs. 3	Datenschutz bei Forschungsvorhaben
Saarland	§ 14 Abs. 2	Forschung und Patientendaten
Sachsen	§ 34 Abs. 2, Abs. 3	Datenschutz bei Forschungsvorhaben

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
Sachsen-Anhalt	§ 17 Abs. 2	Verarbeitung von Patientendaten zu Forschungszwecken
Schleswig-Holstein	§ 38	Verarbeiten von Patientendaten im Rahmen von Forschungsvorhaben
Thüringen	§ 27a	Datenverarbeitung für Forschungszwecke außerhalb des Krankenhauses
Krebsregisterdatengesetz des Bundes (BKRG)		
BKRG	§ 5	Datenübermittlung an das Zentrum für Krebsregisterdaten, Verordnungsermächtigung
BKRG	§ 6	Datenverarbeitung und Datenübermittlung, Mitarbeit in Organisationen
BKRG	§ 7	Zusammenarbeit mit den Krebsregistern
BKRG	§ 8	Datenübermittlung und Datenbereitstellung zu Forschungszwecken
Krebsregistergesetze der Länder (KRG)		
Baden-Württemberg	§ 9	Gesundheitsforschung
Bayern	Art. 13	Datennutzung durch Dritte
Staatsvertrag zwischen den am Gemeinsamen Krebsregister beteiligten Bundesländern Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt, Sachsen, Thüringen	Art. 4a	Datenabgleich mit dem Zentrum für Krebsregisterdaten
Berlin und Brandenburg	Art. 32	Datenübermittlung für die Versorgungsforschung
Bremen	§ 16	Bereitstellung von Daten für Forschungsvorhaben
Hamburg	§ 7-9	Übermittlung aggregierter Daten; Übermittlung anonymisierter Einzeldaten; Übermittlung personenbezogener Daten
Hessen	§ 9	Abgleichung und Übermittlung personenidentifizierender Daten
Mecklenburg-Vorpommern	§ 9	Datenbereitstellung für Forschungszwecke

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
Niedersachsen	§ 20	Datenübermittlung an Dritte zur Qualitätssicherung oder für Forschungszwecke
Nordrhein-Westfalen	§ 23	Allgemeine Auskünfte, Auskünfte für Forschungsvorhaben und zur Gesundheitsberichterstattung
Rheinland-Pfalz	§ 12	Abgleichung und Übermittlung personenidentifizierender Daten
Saarland	§ 13	Abgleichung, Zusammenführung und Übermittlung von Daten für Maßnahmen des Gesundheitsschutzes und Forschungsvorhaben
Sachsen	§ 13	Wissenschaftliche Nutzung der Daten
Sachsen-Anhalt	§ 17	Datenbereitstellung für Forschungszwecke, Studien zur Qualitätssicherung
Schleswig-Holstein	§ 16	Übermittlung klinisch-epidemiologischer Daten
Thüringen	§ 14	Datenbereitstellung für Forschungszwecke
Meldegesetz des Bundes (BMG)		
BMG	§ 44	Einfache Meldeauskunft
BMG	§ 45	Erweiterte Meldeauskunft
BMG	§ 46	Gruppenauskunft
Sozialgesetzbuch (SGB)		
SGB I	§ 35	Sozialgeheimnis
SGB II	§ 51b	Verarbeitung von Daten durch die Träger der Grundsicherung für Arbeitsuchende
SGB III	§ 282 Abs. 5	Arbeitsmarkt- und Berufsforschung
SGB III	§ 394	Verarbeitung von Sozialdaten durch die Bundesagentur
SGB III	§ 395	Datenübermittlung an Dritte; Verarbeitung von Sozialdaten durch nichtöffentliche Stellen
SGB IV	§ 18f	Zulässigkeit der Verarbeitung

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
SGB V	§ 25a Abs. 5	Organisierte Früherkennungsprogramme
SGB V	§ 64e Abs. 10	Modellvorhaben zur umfassenden Diagnostik und Therapiefindung mittels Genomsequenzierung bei seltenen und bei onkologischen Erkrankungen, Verordnungsermächtigung
SGB V	§ 137a Abs. 10	Institut für Qualitätssicherung und Transparenz im Gesundheitswesen
SGB V	§ 287	Forschungsvorhaben
SGB V	§ 287a	Federführende Datenschutzaufsicht in der Versorgungs- und Gesundheitsforschung
SGB V	§ 303b Abs. 3	Wahrnehmung der Aufgaben der Datentransparenz; Verordnungsermächtigung
SGB V	§ 303d	Forschungsdatenzentrum
SGB V	§ 303e	Datenverarbeitung
SGB V	§ 363	Verarbeitung von Daten der elektronischen Patientenakte zu Forschungszwecken
SGB VII	§ 199	Verarbeitung von Daten durch die Unfallversicherungsträger
SGB VII	§ 204	Errichtung eines Dateisystems für mehrere Unfallversicherungsträger
SGB VII	§ 206	Verarbeitung von Daten für die Forschung zur Bekämpfung von Berufskrankheiten
SGB VIII	§ 64 Abs. 2a	Datenübermittlung und -nutzung
SGB X	§ 67 Abs. 2	Begriffsbestimmungen
SGB X	§ 67b	Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten
SGB X	§ 75	Übermittlung von Sozialdaten für die Forschung und Planung
SGB XI	§ 98	Forschungsvorhaben

Gesetz	Einzelvorschrift	Bezeichnung/Beschreibung
SGB XII	§ 119	Wissenschaftliche Forschung im Auftrag des Bundes
Strafgesetzbuch (StGB)		
StGB	§ 203	Verletzung von Privatgeheimnissen

E. Der Forschungsdatenschutz im grenzüberschreitenden Datenverkehr

Für den grenzüberschreitenden Datenverkehr sind Datenübermittlungen innerhalb der Europäischen Union und Datenübermittlungen an Drittländer oder internationale Organisationen, die außerhalb des europäischen Binnenraums liegen, zu unterscheiden.[102] Für den Datentransfer außerhalb des europäischen Binnenraums sind sodann wiederum Datenübermittlungen auf Grundlage eines für das Drittland vorliegenden Angemessenheitsbeschluss und Übermittlungen personenbezogener Daten an sog. unsichere Drittländer, zu unterscheiden.[103] Im Forschungskontext können die Fragen des grenzüberschreitenden personenbezogenen Datenverkehrs vor allem dann relevant sein, wenn Daten z.B. auf im Ausland gehostete Cloud-Dienste übertragen werden oder Forschungspartner innerhalb eines Projekts ihren Sitz im außereuropäischen Ausland haben. Für die entsprechenden Datenübermittlungen sind die nachfolgenden Maßgaben zu beachten. Hierbei gilt, dass allgemeine personenbezogene Daten und besonders sensible Datenkategorien grundsätzlich rechtlich gleichbehandelt werden.

Ob eine Datenübermittlung in Drittländer nach der DS-GVO zulässig ist, erfolgt grundsätzlich in zwei Schritten.[104] Zuerst ist zu prüfen, ob die allgemeinen Rechtmäßigkeitsvoraussetzungen einer Verarbeitung personenbezogener Daten gem. Art. 5 ff. DS-GVO erfüllt sind. An zweiter Stelle ist sodann zu prüfen, ob die Anforderungen an eine Übermittlung personenbezogener Daten an Drittländer nach den Art. 45 ff. DS-GVO erfüllt sind.[105] Dabei stellt sich die Frage, ob eine Datenübermittlung aufgrund eines Angemessenheitsbeschlusses gem. Art. 45 DS-GVO legitimiert ist oder geeignete Garantien gem. Art. 46 DS-GVO vorliegen oder eine der in Art. 49 DS-GVO normierten Ausnahmen einschlägig ist.

I. Datenübermittlung innerhalb des datenschutzrechtlichen Binnenraums

Zum datenschutzrechtlichen Binnenraumen zählen die Mitgliedstaaten der Europäischen Union sowie des Europäischen Wirtschaftsraums. Für diesen Binnenraum gilt ein einheitliches Datenschutzniveau,

[102] *Pauly,* in: Paal/Pauly, DS-GVO BDSG, Art. 44 DS-GVO, Rn. 6.
[103] *Zerdick,* in: Ehmann/Selmayr, DS-GVO, Art. 44, Rn. 14.
[104] *Buchner*, in: Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 281
[105] *Beck,* in: BeckOK-Datenschutzrecht, Art. 44 DS-GVO, Rn. 8, 38 ff; *Zerdick,* in: Ehmann/Selmayr, DS-GVO, Art. 45, Rn. 17.

welches durch die DS-GVO gewährleistet wird. Somit ist der grenzüberschreitende Datentransfer innerhalb der EU und EWR-Staaten einem inländischen Datenaustausch gleichgestellt.[106]

II. Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses

Für Datenübermittlungen in sog. Drittländer oder internationale Organisationen außerhalb des datenschutzrechtlichen Binnenraums besteht die Möglichkeit, Daten auf Grundlage eines Angemessenheitsbeschlusses gem. Art. 45 DS-GVO zu übermitteln. Die Europäische Kommission kann sog. Angemessenheitsbeschlüsse fassen, die feststellen, dass ein bestimmtes Drittland für die Verarbeitung personenbezogener Daten einen mit dem europäischen Datenschutzrecht vergleichbaren adäquaten Schutz gewährleistet. Grundsätzlich muss in diesem Zusammenhang sichergestellt werden, dass das durch die DS-GVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.[107] Soweit ein Angemessenheitsbeschluss vorliegt, ist der Datentransfer grundsätzlich ohne weitere Genehmigung möglich. Die Drittstaaten mit Angemessenheitsbeschluss sind solchen der EU gleichgestellt und bieten demnach ein angemessenes Datenschutzniveau. Für folgende Drittstaaten wurde zurzeit (Stand März 2022) ein solcher Angemessenheitsbeschluss gefasst[108]:

- Andorra
- Argentinien
- Kanada
- Färöer-Inseln
- Guernsey
- Israel
- Isle of Man
- Japan
- Jersey
- Neuseeland
- Republik Korea (Südkorea)
- Schweiz
- Uruguay

[106] *Buchner*, in: Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 277.
[107] *Pauly* in: Paal/Pauly, DS-GVO BDSG, Art. 45 DS-GVO, Rn. 1b.
[108] Der aktuelle Stand der Angemessenheitsbeschlüsse kann auf der Website der Europäischen Kommission eingesehen werden: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (18.03.2022).

- Vereinigtes Königreich

III. Datenübermittlung in unsichere Drittländer

Datenübermittlungen in Drittländer, die nicht zum europäischen Binnenraum gehören und für die auch kein Angemessenheitsbeschluss vorliegt, sind aus datenschutzrechtlicher Sicht als unsicher einzustufen. Eine Datenübermittlung in sog. unsichere Drittländer bedarf demnach besonderer Vorkehrungen gem. Art. 46 DS-GVO, damit die Einhaltung eines angemessenen Datenschutzniveaus gewährleistet werden kann. Die geeigneten Garantien sollen entsprechend Erwägungsgrund 108 der DS-GVO sicherstellen, dass „die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden". Dabei sollen die datenschutzrechtlichen Grundsätze, die Grundsätze des Datenschutzes durch Technik sowie datenschutzfreundliche Voreinstellungen besonders berücksichtigt werden.[109]

Die bislang wichtigste Grundlage für die Legitimation einer Datenübermittlung in Drittländer sind die von der Europäischen Kommission erlassenen Standarddatenschutzklauseln (sog. „SCC"),[110] die zu den genehmigungsfreien Garantien gem. Art. 46 Abs. 2 lit. c DS-GVO zählen. Diese formulieren Vertragstexte, insbesondere die wechselseitigen Rechte und Pflichten, für die an einer Datenübermittlung beteiligten Parteien.[111] Vereinfacht gesprochen werden somit die gesetzlichen Vorgaben aus der DS-GVO in das Vertragswerk zwischen der Daten übermittelnden und der Daten empfangenden Stelle übertragen. Die Standarddatenschutzklauseln wurden durch die EU-Kommission im Juni 2021 als Folge des Schrems-II-Urteils vom 16. Juli 2020[112] umfassend angepasst. Bei neuen Vertragsabschlüssen zum Auslandsdatentransfer sind seit dem 27.09.2021 die aktualisierten Standarddatenschutzklauseln zu verwenden und die Vorgängerregelungen vor dem 27.12.2022 durch diese zu ersetzen. Zusätzlich zu den vertraglichen Regelungen, die durch die SCC getroffen werden, sollten bei einer Datenübermittlung in unsichere Drittländer weitere technisch-organisatorische Schutzmaßnahmen (TOM) vorgesehen werden. Dies gilt insbesondere für die Übermittlung von Gesundheitsdaten und vergleichbaren sensitiven Datenbeständen. Derlei TOM umfassen zuvorderst die Datenverschlüsselung sowie die Anonymisierung.[113]

[109] *Pauly,* in: Paal/Pauly, DS-GVO BDSG, Art. 46 DS-GVO, Rn. 7.
[110] *Lange/Filip,* in: BeckOK-Datenschutzrecht, Art. 46 DS-GVO, Rn. 26.
[111] *Buchner*, in: Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 283.
[112] EuGH ZD 2020, 511.
[113] *Martini,* in: Paal/Pauly, DS-GVO BDSG, Art. 24 DS-GVO, Rn. 20 ff.

F. Bewertung des rechtlichen Status quo und rechtspolitischer Ausblick

Insgesamt ergeben sich mit Blick auf die gegenwärtige Rechtslage erhebliche praktische Probleme bei der Durchführung von Forschungsvorhaben. Diese praktischen Probleme betreffen die Anwendbarkeit unterschiedlicher Datenschutzregeln, die Bereitschaft von Studienteilnehmenden und die Notwendigkeit einer Einwilligung, den organisatorischen Aufwand aufgrund der Vielzahl an Verfahren und Projektbeteiligten, die Zuständigkeiten diverser Aufsichtsbehörden sowie teilweise die Abhängigkeit von Stellungnahmen und Genehmigungsverfahren durch Behörden von Bund und Ländern.

Verschärft wird die allgemeine rechtliche Problematik durch die Tatsache, dass Forschungsprojekte in der Regel in der Form von Forschungskooperationen bzw. Verbundvorhaben organisiert sind und sich hieraus unterschiedlichste Rollen und Verantwortlichkeiten ergeben, so beispielsweise bezogen auf Dateneigner, Datenverarbeiter, Auftragsverarbeiter/gemeinsame Verantwortliche, Treuhandstellen, Datenschutzbeauftragte und Aufsichtsbehörden. Nicht selten sind die Verbundpartner unterschiedlichen Rechtsräumen mit unterschiedlichen (datenschutz)rechtlichen Anforderungen zuzuordnen und es ist zwischen öffentlichen Stellen (z.B. Universitäten und Hochschulen) und privaten Einrichtungen wie Unternehmen und Vereinen zu unterscheiden. Die aufsichts- und fachbehördlichen Kontrollstrukturen haben weitere Unklarheiten zur Folge und bedeuten einen erheblichen Mehraufwand in der Verwaltung von Forschungsdaten.

Umso wichtiger ist es für die Wissenschaft, dass neue Datenverarbeitungstechnologien entwickelt und erprobt werden, die eine anonyme und dennoch effektive Datennutzung zu Forschungszwecken ermöglichen. Von zentraler Bedeutung in diesem Zusammenhang ist auch der einfache und problemlose Austausch von Daten inklusive einer wissenschaftlichen Nachnutzung, insbesondere für den grenzüberschreitenden Datenaustausch. Dies entspricht auch dem Gebot der wissenschaftlichen Forschungsförderung, Datenverarbeitungstechnologien nach dem Stand von Wissenschaft und Technik zu entwickeln.[114]

Eine Harmonisierung des Forschungsdatenschutzes ist insgesamt überfällig. Die damit einhergehende Forderung nach einem Bund-Länder-Staatsvertrag für die medizinische Forschung[115] wurde mittlerweile „zurückgezogen“. Der aktuellste Vorschlag[116] zwecks Beseitigung von Forschungshindernissen und

[114] *Molnár-Gábor/Korbel*, ZD 2016, 274, 275.
[115] https://www.uni-kiel.de/medinfo/documents/TWMK%20Vorschlag%20DInfMedForsch%20v1.9%20170927.pdf (08.03.2022) sowie https://www.netzwerk-datenschutzexpertise.de/dokument/medizinische-forschung-und-datenschutz (08.03.2022), vgl. *Schütze/Krawczak/Weichert*, DANA 4/2017, 185, 193 ff.; *Weichert/Krawczak,* MIBE 2019, Vol. 15(1), 1-8; *Hänold*, ZD-Aktuell 2020, 07046.
[116] Stand 22.02.2021.

Schutzdefiziten findet sich in der Forderung nach einem medizinischen Forschungsgesetz wieder.[117] Außerdem plant die Bundesregierung ein Forschungsdatengesetz, welches den Zugang zu Forschungsdaten für öffentliche und private Forschung verbessern und vereinfachen soll.[118] Daneben ist die Weiterentwicklung der Nationalen Forschungsdateninfrastruktur sowie eines Europäischen Forschungsdatenraums geplant.[119] Außerdem soll zur besseren wissenschaftlichen Nutzung im Einklang mit der DS-GVO ein Registergesetz und Gesundheitsdatennutzungsgesetz auf den Weg gebracht werden.[120]

[117] Netzwerk Datenschutzexpertise, Plädoyer für ein medizinisches Forschungsgesetz, S. 2-11.
[118] Koalitionsvertrag 2021 zwischen SPD, Bündnis 90/Die Grünen und FDP, S. 21.
[119] Koalitionsvertrag 2021 zwischen SPD, Bündnis 90/Die Grünen und FDP, S. 21.
[120] Koalitionsvertrag 2021 zwischen SPD, Bündnis 90/Die Grünen und FDP, S. 83.

Literaturverzeichnis

Autor_in	Titel
AG Consent des Nationalen Steuerungsgremiums der MII des BMBF	Handreichung zur Anwendung der nationalen harmonisierten Patienteninformations- und Einwilligungsdokumente zur Sekundärnutzung von Patientendaten, Version 1.6d vom 16.04.2020, Version 0.9d
Artikel-29-Datenschutzgruppe	Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, 10. April 2018
Dies.	Stellungnahme 5/2014 zu Anonymisierungstechniken, 0829/14/DE WP 216
Deutsches Ärzteblatt	Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, DOI:10.3238./aertzebl.202.ds02
Auer-Reinsdorff, Astrid/Conrad, Isabel (Hrsg.)	Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019
Beck'scher Online-Kommentar zum Datenschutzrecht	Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), 38. Edition, München 2021
Beck'scher Online-Kommentar zum Sozialrecht	Rolfs, Christian/Giesen, Richard/Kreikebohm, Ralf/Meßling, Miriam/Udsching, Peter (Hrsg.), 63. Edition, München 2021
Bischoff, Claudia	Pseudonymisierung und Anonymisierung von personenbezogenen Forschungsdaten im Rahmen klinischer Prüfungen von Arzneimitteln (Teil I) – Gesetzliche Anforderungen, PharmR 2020, 309
Buchner, Benedikt (Hrsg.)	Datenschutz im Gesundheitswesen, Remagen, Stand November 2021
Buchner, Benedikt/Haber, Anna/Hahn, Horst/Kusch, Harald/Prasser, Fabian/Sax, Ulrich/Schmidt, Carsten	Das Modell der Datentreuhand in der medizinischen Forschung, DuD 2021, 806
Bundesbeauftrage für Datenschutz und Informationssicherheit (BfDI)	Positionspapier zur Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche, 2020, verfügbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf (21.03.2022)
Ders.	29. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit, 2020, verfügbar unter:

	https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/29TB_20.html (21.03.2022)
Franzen, Martin/Gallner, Inken/Oetker, Hartmut (Hrsg.)	Kommentar zum europäischen Arbeitsrecht, 4. Aufl., München 2022
Gola, Peter/Heckmann, Dirk (Hrsg.)	Bundesdatenschutzgesetz, 13. Aufl., München 2019
Hänold, Stefanie	KI-Forschung in der Medizin benötigt eine Reform datenschutzrechtlicher Regelungen, ZD-Aktuell 2020, 07046
Herbst, Tobias	Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, DuD 2016, 371
Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.)	Handbuch Multimedia-Recht, 57. Ergänzungslieferung, München 2021
Kasseler Kommentar Sozialversicherungsrecht	Körner, Anne/Leitherer, Stephan/Mutschler, Bernd/Rolfs, Christian (Hrsg.), 117. Ergänzungslieferung, München 2021
Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP	2021
Kühling, Jürgen/Buchner, Benedikt (Hrsg.)	Datenschutzgrundverordnung BDSG, 3. Aufl., München 2020
Leupold, Andreas/Wiebe, Andreas/Glossner, Slike (Hrsg.)	Münchener Anwaltshandbuch IT-Recht, 4. Aufl., München 2021
March, Stefanie/Rauch, Angela/Bender, Stefan/Ihle, Peter	Data protection aspects concerning the use of social or routine data, FDZ-Methodenreport 12/2015 EN, Magdeburg, verfügbar unter: https://doku.iab.de/fdz/reporte/2015/MR_12-15_EN.pdf (07.03.2022)
March, Stefanie/Andrich, Silke/Drepper, Johannes/Horenkamp-Sonntag, Dirk/Icks, Andrea/Ihle, Peter/Kieschke, Joachim/Kollhorst, Bianca/Maier, Birga/Meyer, Ingo/Müller, Gabriele/Ohlmeier, Christoph/Peschke, Dirk/Richter, Adrian/Rosenbusch, Marie-Luise/Scholten, Nadine/Schulz, Mandy/Stallmann, Christoph/Swart, Enno/Wobbe-Ribinski, Stefanie/Wolter, Antke/Zeidler, Jan/Hoffmann, Falk	Gute Praxis Datenlinkage (GDP), Gesundheitswesen 2019, 81, S. 636, verfügbar unter: https://www.thieme-connect.com/products/ejournals/pdf/10.1055/a-0962-9933.pdf (08.03.2022)
Molnár-Gábor, Fruzsina/Korbel, Jan	Verarbeitung von Patientendaten in der Cloud

	Die Freiheit translationaler Forschung und der Datenschutz in Europa, ZD 2016, 274
Netzwerk Datenschutzexpertise	Plädoyer für ein medizinisches Forschungsgesetz, Stand 22.02.2021
Paal, Boris/Pauly, Daniel (Hrsg.)	Datenschutzgrundverordnung Bundesdatenschutzgesetz, 3. Aufl., München 2021
Rat für Soziales- und Wirtschaftsdaten	Handreichung Datenschutz, 2. vollständig überarbeitete Auflage. RatSWD Output 8 (6), Berlin 2020
Roßnagel, Alexander	Datenschutz in der Forschung – Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen, ZD 2019, 157
Roßnagel, Alexander/ Geminn, Christian	Vertrauen in Anonymisierung – Regulierung der Anonymisierung zur Förderung Künstlicher Intelligenz, ZD 2021, 487
Schaar, Katrin	DS-GVO: Geänderte Vorgaben für die Wissenschaft Was sind die neuen Rahmenbedingungen und welche Fragen bleiben offen?, ZD 2016, 224
Schütze, Bernd/Krawczak, Michael/Weichert, Thilo	Datenschutznachrichten (DANA) – Gesundheitswesen 4/2017, 185
Specht, Louisa/Mantz, Reto (Hrsg.)	Handbuch Europäisches und deutsches Datenschutzrecht – Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, München 2019
Spindler, Gerald/Schuster, Fabian (Hrsg.)	Recht der elektronischen Medien, 4. Aufl., München 2019
Sydow, Gernot (Hrsg.)	Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018
Taeger, Jürgen/Gabel, Detlev (Hrsg.)	DS-GVO – BDSG – TTDSG, 4. Aufl., Frankfurt am Main 2022
Taeger, Jürgen/Pohle, Jan (Hrsg.)	Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 36. Ergänzungslieferung, München 2021
Tinnefeld, Marie-Theres/Buchner, Benedikt/Petri, Thomas/Hof, Hans-Joachim	Einführung in das Datenschutzrecht, 7. Aufl., Berlin/Boston 2019
Weichert, Thilo	Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung – Vorgaben der EU-Datenschutzgrundverordnung und national geltender Gesetze, Berlin 2022

Ders.	Die Forschungsprivilegierung in der DS-GVO – Gesetzlicher Änderungsbedarf bei der Verarbeitung personenbezogener Daten für Forschungszwecke, ZD 2020, 18
Weichert, Thilo/Krawczak, Michael	Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland, GMS Medizinische Informatik, Biometrie und Epidemiologie (MIBE); VOL: 15 (1); DOC03 /20190327/