Prof. Dr. Louisa Specht-Riemenschneider

im Auftrag des Bundesministeriums für Bildung und Forschung

„Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität“

August 2021

Inhaltsverzeichnis

I. Einleitung

„Gesellschaft braucht Wissenschaft – Wissenschaft braucht Daten".[1] Der Zugang zu Daten für Forschung und Wissenschaft ist Grundbedingung wissenschaftlichen Erkenntnisgewinns, auch und gerade im gesamtgesellschaftlichen Interesse. Er hilft im Gesundheitssektor beispielsweise, Nebenwirkungen von Medikamenten oder Impfungen zu erkennen und Therapiemöglichkeiten zu verbessern. Nur der Zugang zu Datenbeständen von Plattformen im Online-Wirtschaftssektor erlaubt Forschung und Wissenschaft die Untersuchung eingesetzter Algorithmen z.B. im Hinblick auf Diskriminierungsfragen, potentielles Overblocking, die Verbreitung von Desinformation oder auch die angewandten Praktiken, um Nutzer zu einer bestimmten Entscheidung zu bewegen. Spotify beispielsweise hat eine Spracherkennungs-Software entwickelt, mit deren Hilfe Empfehlungen für Songs oder Anzeigen ausgesprochen werden können, die von der Stimmung des Nutzers abhängen.[2] Dies hat zumindest das Potential, Fehlkäufe infolge eines projection bias herbeizuführen.[3] Im Mobilitätssektor lassen sich über einen verbesserten Datenzugang für die Forschung intelligente Verkehrssysteme entwickeln und evaluieren. Im Energiesektor könnte durch die Analyse von Stromverbrauchszahlen und -faktoren die Energieeffizienz steigen.

Fehlender Forschungsdatenzugang wird zunehmend vor allem in jüngster Zeit beklagt.[4] Bereits *Havel* forderte aber in seiner Dissertationsschrift „Informationszugangsansprüche des forschenden Wissenschaftlers" aus dem Jahr 2015 die Schaffung eines flächendeckenden Anspruchs auf Informationszugang zugunsten von Forschung und Wissenschaft[5] und *Wielsch* entwickelte in seiner Habilitationsschrift „Zugangsregeln – Die Rechtsverfassung der Wissensteilung" medienspezifische Zugangsregeln zu geistigen Schutzgütern.[6] Auf den in diesen Arbeiten entwickelten Gedanken soll im Rahmen dieser Studie aufgebaut werden. Auch die Kommission Wettbewerbsrecht 4.0 sprach sich – wenn auch knapp – für einen Forschungsdatenzugang zugunsten der Forschung aus.[7]

Der Zugang zu sozial-, verhaltens- und wirtschaftswissenschaftlichen Forschungsdaten beruht in Deutschland de lege lata im Wesentlichen auf einem System von 39 Forschungsdatenzentren, die

---

[1] Leitmotiv der 8. Konferenz für Sozial- und Wirtschaftsdaten des Rates für Sozial- und Wirtschaftsdaten (RatSWD) 2020.
[2] *Savage*, Spotify wants to suggest songs based on your emotions, abrufbar unter: https://www.bbc.com/news/entertainment-arts-55839655, zuletzt abgerufen am 16.07.2021.
[3] *Heidhues/Köster/Köszegi*, Steering Fallible Consumers, 2021, S. 10-11, abrufbar unter: http://www.personal.ceu.hu/staff/Botond_Koszegi/steering.pdf, zuletzt abgerufen 16.07.2021.
[4] *Peichl/Bachmann/Riphahn*, FAZ v. 06.08.2021, abrufbar unter: https://www.faz.net/aktuell/wirtschaft/forschern-stehen-in-deutschland-zu-wenige-daten-zur-verfuegung-17471899.html, zuletzt abgerufen am 20.08.2021; anders noch die Bestandsaufnahme im Jahr 2015 von *Hevers*, Informationszugangsansprüche des forschenden Wissenschaftlers, S. 470 f., der aber darauf hinweist, dass dies wohl der Tatsache geschuldet ist, dass zum damaligen Zeitpunkt viele Daten auf freiwilliger Grundlage zur Verfügung gestellt wurden.
[5] *Havel*, Informationszugangsansprüche des forschenden Wissenschaftlers, S. 453.
[6] *Wielsch*, Zugangsregeln – Die Rechtverfassung der Wissensteilung.
[7] Abschlussbericht, S. 46.

durch den Rat für Sozial- und Wirtschaftsdaten (Rat SWD) akkreditiert werden. Im Rahmen der Nationalen Forschungsdateninfrastruktur sollen diese nationalen Forschungsdatenzentren gestärkt werden, ohne das System als föderale Infrastruktur aber aufzugeben. Die Zugangswege in den Forschungsdatenzentren sollen beispielsweise transparenter und einheitlicher gestaltet werden, es soll ein landesweites Netz von Zugangspunkten (z.B. Gastwissenschaftler-Arbeitsplätze) sowie eine föderierte Archivierungsinfrastruktur aufgebaut werden.[8] Die Zugangsgewährung über Forschungsdatenzentren ist wichtige Grundlage empirischer Forschung, gleichwohl steht sie nicht im Zentrum dieser Studie. Die hier vorgenommene Untersuchung richtet sich vielmehr v.a. auf die Gewährleistung von Zugang zu denjenigen bei öffentlichen und privaten Stellen anfallenden Daten, die de lege lata nicht bereits in Forschungsdatenzentren gespeichert werden, weil diese Daten für die untersuchten Sektoren besondere Relevanz haben. Die Forschungsdatenzentren ließen sich aber in die im Rahmen dieser Studie entwickelten Datenzugangsökosysteme eingliedern.

Materiell-rechtlich kann Datenzugang auf verschiedenen Wegen gewährleistet werden: Vertragliche Auskunftsansprüche führen ebenso zu einem Datenzugang wie die Ausübung datenschutzrechtlicher Befugnisse.[9] Auch kartellrechtliche Zugangsansprüche existieren.[10] All diese Zugangsansprüche gelten allerdings nicht vorrangig der Wissenschaft, zugangsberechtigt können vielmehr auch und gerade nicht wissenschaftlich tätige Personen sein. Im Fokus dieser Studie stehen aber explizit Forschungsklauseln, die einen privilegierten Zugang von Wissenschaft und Forschung normieren. Unspezifische Zugangsansprüche werden damit als Untersuchungsgegenstand vernachlässigt.

Abseits vertraglicher, datenschutzrechtlicher und kartellrechtlicher Verpflichtungen wird Datenzugang allerdings bislang äußerst rudimentär gewährt. Klauseln, die Datenzugang für die Forschung erlauben oder zu ihm verpflichten (Forschungsklauseln) finden sich nur vereinzelt, z.B. in § 19 Abs. 3 Urheberrechts-Diensteanbieter-Gesetz (UrhDaG), in § 5a Netzwerkdurchsetzungsgesetz (NetzDG), in § 8 des Entwurfs des Bundeskrebsregistergesetzes oder in § 303e SGB V. Die jeweils vom Zugangsanspruch umfassten Daten sind darüber hinaus limitiert, die Zugangsvoraussetzungen ganz unterschiedlich ausgestaltet. Nach Art. 31 des Entwurfs des Digital Services Acts (DSA-E) soll Forschern Datenzugang beispielsweise nur über eine Drittinstanz mit behördlicher Struktur erteilt werden können. Ein ähnliches Modell findet sich in Finnland mit Blick auf Gesundheitsdaten. Hier wurde eine nationale Behörde (Findata) eingerichtet, die den Forschungsdatenzugang koordiniert. Entsprechende Ansätze finden sich auch in Australien. Australien und Großbritannien versuchen darüber hinaus, einen verbesserten Zugang zu Daten auch im wissenschaftlichen Interesse über sogenannte Data Hubs zu gewährleisten, in denen Daten aggregiert und angereichert werden. Insgesamt ist die Landschaft der

[8] https://www.konsortswd.de/konsortswd/tasks/datenzugang/, zuletzt abgerufen am 16.07.2021.
[9] *Specht-Riemenschneider*, Data access rights - A comparative perspective, in: Bundesministerium der Justiz und für Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb, Data Access, Consumer Interests and Public Welfare, 2021, S. 402 ff.
[10] Dazu umfassend: *Podszun*, Handwerk in der digitalen Ökonomie, S. 76 ff.

Datenzugangsmöglichkeiten für Wissenschaft und Forschung und die Datenzugangsinfrastruktur, in denen und mit deren Hilfe Datenzugang gewährt wird, äußerst heterogen. Diese Heterogenität nimmt zu, je weiter der Sektorübergriff der Betrachtung ausfällt.

Ziel dieser Studie ist es, die nationalen Datenzugangsmöglichkeiten und die nationale Datenzugangsinfrastruktur ebenso wie die Datenzugangsmöglichkeiten und die Datenzugangsinfrastruktur ausgesuchter fremder Rechtsordnungen zu analysieren, Best-Practice-Regelungen zu identifizieren und zu ergänzen und daraus funktionierende Datenzugangsökosysteme zu entwickeln. Datenzugangsinfrastruktur und Datenzugangsansprüche sind unbedingt auf diese Weise zusammen zu denken, denn der beste Datenzugangsanspruch hilft nicht, wenn er letztlich aufgrund fehlender Datenzugangsinfrastrukturen nicht ausgeübt wird. Die beste Datenzugangsinfrastruktur hilft nicht, wenn die Regeln der Datenzugangsgewährung fehlen. Darüber hinaus können über die Datenzugangsinfrastruktur auftretende Konflikte zwischen den betroffenen Rechten und Interessen von Datenzugangsberechtigten (für die die Forschungsfreiheit streitet), Datenzugangsverpflichteten (bei denen insb. der Geschäftsgeheimnisschutz sowie Datenbankschutzrechte betroffen sein dürften) und Drittbetroffenen (bei denen durch den Datenzugang das informationelle Selbstbestimmungsrecht berührt sein kann) aufgelöst werden, indem die Daten beispielsweise ausschließlich in gesicherten Umgebungen eines Datentreuhänders zugänglich gemacht oder vor einer Zugangsverschaffung von diesem anonymisiert oder pseudonymisiert werden. Auch die Art und Weise der Datenzugangsverschaffung und des Umgangs mit den vom Datenzugang betroffenen Daten (Nachnutzungsregelungen) können entsprechend risikomindernd ausgestaltet werden.

Die Entwicklung dieser Datenzugangsökosysteme wird sektorspezifisch erfolgen, um eine größtmögliche Passgenauigkeit im Hinblick auf die sektorspezifisch berührten Rechte und Interessen der vom Datenzugang betroffenen Personen zu erreichen. Untersucht werden die Sektoren Gesundheit, Online-Wirtschaft (im Wesentlichen Online-Plattformen), Mobilität und Energie, die auftraggeberseitig vorgegeben sind. Aufgrund ihres besonderen Fortschritts in der Datenzugangsgewährung für Forschung und Wissenschaft werden die Rechtsordnungen der Staaten Finnland, Kanada, Australien, Frankreich, Großbritannien und Indien analysiert.

Best-Practice Beispiele für den Gesundheitssektor finden sich insb. im My Health Records Act (2012) in Australien, auf Ebene der kanadischen Provinzen in der General Directive - Access to Health Data for Research, British Columbia (2018), in Finnlands Act on the Secondary Use of Health and Social Data (2019) sowie in Frankreichs Code de la santé publique (2018). Großbritannien gewährt Datenzugang für Wissenschaft und Forschung über sogenannte Research Data Hubs.

Für den Mobilitätssektor wurde im australischen New South Wales durch das Ministry of Transport eine Plattform (Transport for NSW – Open Data Hub) eingerichtet, über die staatliche Daten sowie Drittdaten durch Vertrag zugänglich gemacht werden. Auch Akteure aus der Wissenschaft können dabei Vertragspartner sein, Zweck ist explizit auch und gerade „Policy Research".[11] Vorrangig Australien soll daher im Mobilitätssektor als best-practice erörtert werden.

Im Energiesektor ist eine entsprechende Plattform auch in Großbritannien vorgesehen. Nachdem eine „Energy Data Task Force"[12] entsprechende Empfehlungen ausgearbeitet hat, entwickelt Siemens die nationale Energiedatenplattform „Yoda" (Your Online Digital Architecture), über die Energiedaten zugänglich gemacht werden können. Auch zu derartigen Plattformen kann der Datenzugang für Wissenschaft und Forschung privilegiert ausgestaltet werden. Vorrangig Großbritannien soll daher mit Blick auf den Energiesektor als best-practice betrachtet werden.

Da für die Sektoren Mobilität, Energie und Online-Wirtschaft die bereits existenten Datenzugangsansprüche weniger vielzählig sind, soll methodisch der Gesundheitssektor zum Ausgangspunkt der Untersuchung gemacht werden, die drei übrigen Sektoren sollen im Anschluss erörtert werden. Im Rahmen der Übertragung von Best-Practice-Beispielen in das nationale/europäische Recht kann und soll sektorübergreifend gelernt werden, d.h. dass z.B. nationale/europäische Regelungen für den Energiesektor durchaus Strukturen übernehmen können, die international für den Forschungsdatenzugang im Gesundheitsbereich vorgesehen sind, sofern die Sektorspezifika dies erlauben.

Aus dem derzeit diskutierten Bedarf an Datenzugangsregeln im Bereich B-B, G-B und C-B, die durch den für das vierte Quartal 2021 angekündigten Entwurf eines Data Acts adressiert werden sollen,[13] wird mit dem Forschungsdatenzugang lediglich ein Ausschnitt des erforderlichen Datenzugangsregimes thematisiert. Gleichwohl können die hier erarbeiteten Datenzugangsökosysteme auch herangezogen werden, um als Infrastruktur für noch zu ergänzende Datenzugangsansprüche anderer Akteure, z.B. Wettbewerber, staatliche Akteure etc. zu dienen. Die Datenzugangsansprüche selbst müssen aber freilich für jeden Akteur selbständig unter Abwägung aller relevanten Einzelfallumstände entwickelt werden.

[11] https://opendata.transport.nsw.gov.au/open-data, zuletzt abgerufen am 16.07.2021.
[12] https://www.gov.uk/government/groups/energy-data-taskforce, zuletzt abgerufen am 16.07.2021.
[13] Inception Impact Assessment v. 28.05.2021 zum geplanten Data Act der EU-Kommission, abrufbar unter: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en, zuletzt abgerufen am 16.07.2021.

II. Gang der Untersuchung

Die Ergebnisse dieser Studie sind den nachfolgenden Ausführungen vorangestellt (III.). Anschließend werden die Prinzipien eines Forschungsdatenzugangs identifiziert (IV.) und der grundrechtliche und kompetenzrechtliche (V.) sowie der datenschutzrechtliche Rahmen (VI.) abgesteckt. Anschließend werden die Mittel der Datenzugangsgewährung (Datenzugangsansprüche, Open-Data-Gesetzgebung, Transparenz- und Berichtspflichten, Erlaubnisse der Datenzugangsgewährung) identifiziert und geordnet. Im Mittelpunkt dieser Untersuchung stehen dabei aufgrund ihrer Wirkintensität zugunsten von Wissenschaft und Forschung Datenzugangsansprüche. Die de lege lata bestehenden Datenzugangsansprüche auf nationaler (VII. und VIII.) und internationaler (IX.) Ebene sollen nicht nur mit Blick auf ihre Regelungsstruktur, sondern auch anhand ihrer Voraussetzungen und Rechtsfolgen sowie der Möglichkeiten ihrer Rechtsdurchsetzung geordnet und analysiert werden. Es folgt eine Analyse der Datenzugangsinfrastrukturen, insb. möglicher Datentreuhandsysteme, die als zentrale, dezentral-zentrale oder gänzlich dezentrale Datenspeicher oder aber als bloße Zugangsmittler in einem Datenzugangsökosystem agieren könnten (X.). Die Frage von Standardisierung und Interoperabilität wird als zentrale Voraussetzung eines solchen Datenzugangsökosystems gesondert adressiert (XI.) Die Untersuchung mündet in die Ausgestaltung von Leitlinien für den Forschungsdatenzugang, die in einem Forschungsdatenzugangsgesetz für den Gesundheitssektor sowie einer Musterforschungsdatenklausel für den Online-Wirtschaftssektor ihren Niederschlag finden (XII.) Für den Mobilitätssektor und den Energiesektor sind Forschungsstand und best-practice Lösungen weit weniger fortgeschritten als im Gesundheits- und im Online-Wirtschaftssektor, weshalb die Vorschläge für diese Sektoren deutlich weniger weit reichen können. Die Untersuchung schließt mit 15 rechtspolitischen Handlungsempfehlungen für einen Forschungsdatenzugang (XIII.).

III. Studienergebnisse

1. Daten können hinsichtlich ihrer Zugänglichkeit in vier Zuständen beschrieben werden: Offen, Öffentlich, Gemeinsam genutzt und geschlossen. Für Daten der öffentlichen Verwaltung ist ein Wechsel dieses Zustands von geschlossen (closed data) zu offen (open data) oder öffentlich (public data) erforderlich (der bereits angelaufen ist) für privat gehaltene Daten von geschlossen zu gemeinsam genutzt (shared data).

2. Die Maßstäbe eines Datenzugangs sollten sich insgesamt am „Five Safes Model" orientieren, das Datenzugang in ein Spektrum von fünf Risikodimensionen einordnet, die sich gegenseitig beeinflussen und denen in der gesetzlichen Ausgestaltung des Datenzugangs zu begegnen ist.

3. Datenzugang sollte sich darüber hinaus an den FAIR-Prinzipien orientieren. Daten sollten auffindbar (findable), zugänglich (accessible), interoperabel (interoperable) und wiederverwendbar (reusable) sein.

4. Grundrechtlich sind bei der Ausgestaltung von Datenzugangsrechten sowohl die Rechtspositionen des Datenzugangsadressaten, die Grundrechte Drittbetroffener sowie die grundrechtlichen Interessen der Zugangssuchenden zu berücksichtigen. Sie sind in einen angemessenen Ausgleich zu bringen. Auf Seiten des Datenzugangsadressaten sind v.a. der – je nach vertretener Auffassung – in Art. 12 respektive Art. 14 GG sowie – wiederum je nach vertretener Ansicht[14] - in Art. 17 GRCh bzw. Art. 6, 15, 16 GRCh verankerte Geschäftsgeheimnisschutz berührt, ebenso der in Art. 14 GG und Art. 17 GRCh normierte Schutz des Geistigen Eigentums, z.B. der urheberrechtliche Datenbankschutz nach § 2 UrhG aber auch das sui generis Recht des § 87a UrhG sowie der Schutz der Berufsfreiheit insgesamt zu berücksichtigen. Auf Seiten der von einem Datenzugang Drittbetroffenen ist v.a. das informationelle Selbstbestimmungsrecht, Art. 2 Abs. 1, 1 Abs. 1 GG bzw. Art. 7 und 8 GRCh zu beachten und auf Seiten der Zugangssuchenden die Freiheit von Forschung und Wissenschaft gem. Art. 5 Abs. 3 bzw. Art. 13 GRCh.

5. Der Eingriff in die Rechtspositionen der Datenzugangsadressaten verfolgt mit der Gewährung der Tätigkeit von Forschung und Wissenschaft einen legitimen Zweck. Im Rahmen der Geeignetheit hat der Gesetzgeber traditionell einen sehr weiten Einschätzungsspielraum, der im Falle einer Gewährung des Datenzugangs zugunsten von Forschung und Wissenschaft nicht überschritten sein dürfte.

[14] *Wollenschläger*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Art. 17 GRC Rn. 16; *Wollenschläger*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Art. 16 GRC Rn. 8; *Aplin*, Right to Property and Trade Secrets, in: Geiger, Research Handbook on Human Rights and Intellectual Property, 2015, S. 421-437; *Breuer*, Staatliche Berufsregelung und Wirtschaftslenkung, in Isensee/Kirchhof, Handbuch des Staatsrechts: Band VIII, Grundrechte: Wirtschaft, Verfahren, Gleichheit, 3. Auflage, 2010, § 171 Rn. 38.

6. Eine Gesetzgebungskompetenz der EU für den Forschungsdatenzugang lässt sich aus der Binnenmarktkompetenz, Art. 114 AEUV ableiten, eine Bundeskompetenz aus Art. 74 Abs. 1 Nr. 13 i.V.m. Art. 72 Abs. 2 GG.

7. Datenschutzrechtlich ist ein Forschungsdatenzugang schon de lege lata möglich, vereinzelt sind aber aus Gründen der Rechtssicherheit Klarstellungen im Rechtsrahmen wünschenswert.

8. Ein Datenzugang für die Wissenschaft unabhängig von bereits bestehenden vertraglichen Beziehungen, theoretisch denkbaren kartellrechtlichen Ansprüchen und ebenfalls unabhängig von datenschutzrechtlichen Betroffenenrechten des einzelnen Wissenschaftlers kann über fünf strukturell verschiedene Regulierungsinstrumente mit unterschiedlicher Wirkintensität erreicht werden, nämlich durch

- einen grundrechtsunmittelbaren Datenzugangsanspruch zugunsten der Forschung
- echte Forschungsklauseln
- Open-Data-Gesetzgebung
- Transparenzregelungen und Berichtspflichten
- Erlaubnisse der Datenzugangsgewährung

9. Ein grundrechtsunmittelbarer Datenzugangsanspruch zugunsten der Forschung wird de lege lata überwiegend abgelehnt. Weder die Informationsfreiheit gewährt einen Anspruch auf die Eröffnung von Informationsquellen, noch die Forschungsfreiheit.

10. Die Open-Data Gesetzgebung ist auf einem guten Weg, die Ausweitung des § 12a EGovG ist zu begrüßen. Ansprüche auf Zugang zu bestimmten Daten staatlicher Stellen ergeben sich aus IFG, UIG und VIG und entsprechender landesrechtlicher Regelungen. Die Ansprüche stehen jedermann und damit auch Forschung und Wissenschaft zu. Ein eigener Anspruch aus § 12a EGovG ergibt sich jedoch nicht.

11. Transparenz- und Berichtspflichten wirken nur unzureichend zugunsten von Wissenschaft und Forschung, Erlaubnisse der Datenzugangsgewährung normieren lediglich die datenschutzrechtliche Rechtsgrundlage für die Zugangsgewährung, normieren aber keinen Anspruch auf Forschungsdatenzugang.

12. Datenzugang für die Forschung in den in dieser Studie untersuchten Sektoren ließe sich am effektivsten durch die Verankerung echter Forschungsklauseln, d.h. subjektiver Rechte auf Datenzugang, gewährleisten. Hierbei ist zu unterscheiden zwischen privatrechtlichen und öffentlich-rechtlichen Forschungsklauseln, d.h. solchen Klauseln, die eine private Stelle als Zugangsadressaten definieren und solchen, die eine öffentlich-rechtliche Stelle adressieren.

13. Wird Datenzugang gegenüber privaten Stellen durch ein subjektives Recht auf Datenzugang gewährt, lässt sich diese Forschungsklausel abgeleitet oder originär ausgestalten. Abgeleitet ist sie, wenn sie an bestehende Datenzugangsansprüche angelehnt wird, die Forschung also dem bereits gesetzlich privilegierten Zugangsadressaten gleichgestellt wird, so wie dies z.B. bei § 19 Abs. 3 UrhG der Fall ist. Originär ist das subjektive Recht auf Datenzugang, wenn es ohne Anlehnung an einen anderen Zugangsadressaten einen Datenzugangsanspruch zugunsten der Wissenschaft begründet, wie dies etwa bei § 5a NetzDG der Fall ist. Auch Art. 31 DSA-E enthält eine originäre Forschungsklausel.

14. Echte Forschungsklauseln, die gegen Stellen des öffentlichen Rechts gerichtet sind, müssen außerdem unterschieden werden in gebundene Entscheidungen und Ansprüche auf ermessensfehlerfreie Entscheidungen, wobei die Forschungsfreiheit bei der Ermessensentscheidung zu berücksichtigen ist.

15. Bei der Analyse der de lege lata auf nationaler Ebene existierenden Forschungsklauseln ergibt sich folgendes Bild:

a) Forschungsklauseln existieren de lege lata in den Sektoren Online-Wirtschaft, Gesundheit und Mobilität, nicht aber im Energiesektor. Die Forschungsklauseln im Bereich Archivwesen/Verwaltung kommen hinzu, die in Anbetracht des Untersuchungsgegenstands (Forschungsdatenzugang in den Sektoren Gesundheit, Online-Wirtschaft, Mobilität, Energie) aber nicht vertieft werden.

b) Es lässt sich insgesamt ein sehr enger Anwendungsbereich der existenten Datenzugangsansprüche beobachten, der zweifach spezifiziert ist, nämlich erstens mit Blick auf die erfassten Daten und zweitens mit Blick auf die Zugangsadressaten. Es existiert kein sektorübergreifender Datenzugangsanspruch für Forschung und Wissenschaft, sondern es existieren wenige und zudem äußerst beschränkte sektorspezifische Datenzugangsansprüche.

c) Sind Datenzugangsansprüche gegen öffentlich-rechtliche Stellen gerichtet, existiert ein Ermessensspielraum des Zugangsadressaten jedenfalls im Gesundheitssektor umso eher, je größer das Risiko des Datenzugangs für das informationelle Selbstbestimmungsrecht des von der Datenverarbeitung Betroffenen ausfällt. Je höher die Schutzvorkehrungen z.B. durch Anonymisierungslösungen ausfallen, desto eher kommt es in der Rechtsfolge zu einer gebundenen Entscheidung. Eine solche gebundene Entscheidung ist aus Sicht der Forschung zu bevorzugen. Die Schutzvorkehrungen sollten insofern entsprechend hoch ausfallen, um eine gebundene Entscheidung rechtfertigen zu können. Im Mobilitätssektor hingegen besteht ein Ermessen auch im Falle des Zugangs zu nicht-personenbezogenen Daten. Dies ist zu erklären mit potentiell konfligierenden anderen Rechtspositionen, z.B. des Geschäftsgeheimnisschutzes. Sind Datenzugangsansprüche gegen private Stellen gerichtet, wird die Wahrung von Rechten und Interessen Dritter v.a. durch die Schrankenbestimmungen der Anspruchsnorm gewährleistet.

d) Der kommerzielle Charakter wissenschaftlicher Forschung führt nicht normübergreifend zu einem Ausschluss der Anspruchsberechtigung.

e) Viele – jedoch nicht sämtliche – Forschungsklauseln fordern eine im öffentlichen Interesse, z.T. auch eine im Gemeinwohlinteresse liegende Forschung. Dies lässt sich grundrechtsdogmatisch erklären: Das Gemeinwohlinteresse ist ein besonders schwerwiegendes öffentliches Interesse und ist daher grundrechtsdogmatisch besonders geeignet, um die mit einem Forschungsdatenzugang verbundenen Eingriffe in die Grundrechte der Zugangsadressaten zu rechtfertigen. Je eher das Gemeinwohlinteresse auch durch kommerzielle Forschung erreicht werden kann, desto eher lässt sich auch diese über die Forschungsklauseln als anspruchsberechtigt erfassen.

f) Zusätzliche Antragsvoraussetzungen werden nur von wenigen Forschungsklauseln vorgegeben. Wo sie aber vorgesehen sind, z.B. in Form eines bei Antragstellung vorzulegenden Schutzkonzeptes dienen sie dem Schutz der Grundrechte und Grundfreiheiten Dritter oder des Zugangsadressaten.

g) Ein bei Antragstellung vorzulegendes Schutzkonzept hat höhere Anforderungen zu erfüllen, je höher die durch den Datenzugang entstehenden Risiken für die Grundrechte des Zugangsadressaten oder Dritter ausfällt. Schutzkonzepte sind daher auch und gerade im Interesse von Forschung und Wissenschaft unbedingt zu empfehlen. Denn je geringer die Risiken für die Rechte und Interessen der von einem Datenzugang Betroffenen ausfallen, desto weiter darf der Datenzugangsanspruch im Sinne des Five Safes Models reichen.

h) Der Datenzugang zugunsten von Wissenschaft und Forschung wird de lege lata in der Mehrzahl der Forschungsklauseln nicht unbeschränkt gewährleistet, sondern wird durch Schrankenregelungen begrenzt. Auch dies ist Ausdruck eines Ausgleichs der verschiedenen Grundrechtspositionen von Anspruchsberechtigten, Anspruchsverpflichteten und Dritten.

i) Die Schrankenregelungen der Forschungsklauseln fallen geringer aus, je eingeschränkter der Anwendungsbereich der Forschungsklausel ausgestaltet ist und je weitreichender die Anforderungen an ein bei Antragstellung vorzulegendes Schutzkonzept ausfallen. Dies findet seine Begründung darin, dass bereits auf Ebene von Anwendungsbereich, Antragsgestaltung und Schutzkonzept den Grundrechten der Zugangsadressaten und der Dritten weitreichend Rechnung getragen wird, sodass die Schrankenregelungen selbst eingeschränkter ausfallen können.

j) Eine Reihe an Forschungsklauseln bindet den Datenzugang an den Zweck der (wissenschaftlichen) Forschung. Eine Zweckbindung des Datenzugangs bedeutet, dass diese Daten zunächst allein für die benannten Zwecke, z.B. zur Durchführung wissenschaftlicher Forschungsvorhaben genutzt werden dürfen. Alternativ oder auch kumulativ finden sich Regelungen der Anschlussnutzung, die sowohl die

Ausgangsdaten betreffen können (etwa Anonymisierung nach Abschluss des Forschungsvorhabens; zweckändernde Anschlussnutzung) als auch die Forschungsergebnisse.

k) Weitere Voraussetzungen des Datenzugangs finden sich in einigen Forschungsklauseln im Kriterium der Erforderlichkeit, z.T. wird auch ein „besonders begründeter Fall“ als Einschränkung vorgesehen, wieder andere Forschungsklauseln sehen eine Beteiligung eines wissenschaftlichen Ausschusses bei der Entscheidung über den Datenzugang vor. Auch all diese zusätzlichen Voraussetzungen haben gemein, dass sie den Datenzugang für Wissenschaft und Forschung einschränken, um dadurch einen Ausgleich mit kollidierenden Rechtspositionen zu gewährleisten, indem weitere „Safeguards“ zur Wahrung dieser kollidierenden Rechte vorgesehen werden. Diese „Safeguards“ können materiell-rechtlich (durch das Kriterium der Erforderlichkeit) oder formell (durch die Beteiligung von Gremien am Entscheidungsprozess) gewährleistet werden.

l) Im Gesundheitssektor findet sich eine umfassende Regelung der Datenzugangsvergütung in der Datentransparenz-Gebührenverordnung, die für die Datenzugangsgewährung nach den §§ 303a ff. SGB V gilt.

m) Im Online-Wirtschaftssektor existieren Vergütungsregelungen jedenfalls im nationalen Recht in Form eines Anspruchs auf Erstattung der durch den Datenzugang entstehenden Kosten in angemessener Höhe. Dies ist Ausdruck eines angemessenen Ausgleichs des durch den Datenzugang entstehenden Aufwandes. Vergütungsansprüche sind geeignet, den Datenzugang für Forschung und Wissenschaft unattraktiv auszugestalten und Datenzugang faktisch zu erschweren. § 5a NetzDG sieht daher vor, dass die Kosten kein wesentliches Hindernis für die Inanspruchnahme des Datenzugangsanspruchs darstellen dürfen. Sie bestimmen sich nach § 287 Abs. 1 ZPO. Außerdem gilt eine Höchstgrenze von 5.000 Euro.

n) Innerhalb welcher Frist Datenzugang zu gewähren ist, wird durch die untersuchten Forschungsklauseln kaum vorgegeben. Einzig der DSA-Entwurf enthält die Vorgabe, dass der Datenzugang innerhalb einer „angemessenen Frist“ zu gewährleisten ist. Jedenfalls für die öffentlich-rechtlichen Zugangsregelungen, die in der Rechtsfolge eine Ermessensentscheidung vorsehen, kann außerdem auf die allgemeinen Grundsätze zurückgegriffen werden, wonach eine ordnungsgemäße Ermessensausübung eine Zugangsgewährung in angemessener Zeit erfordert. Datenzugangsbegehren können sehr unterschiedlich im Umfang und auch in der Dringlichkeit ausfallen, weshalb die Normierung genereller Fristen ausscheiden dürfte. Andererseits muss der Forscher aber einen Anhaltspunkt haben, ab welchem Zeitpunkt er ohne das Risiko eines sofortigen Anerkenntnisses mit negativer Kostenfolge für ihn Klage erheben kann. Will man nicht dem Forscher abverlangen, jeweils im Einzelfall Fristen zu setzen, wird man daher um eine gleichermaßen variable wie präzise Fristsetzung nicht herumkommen. In Betracht kommen etwa Formulierungen wie „unverzüglich“ bei gleichzeitiger

Normierung einer Höchstgrenze. Gleichermaßen ist aber darauf zu achten, dem Datenzugangsadressaten die Möglichkeit der Fristverlängerung in Abhängigkeit von Art und Umfang des Datenzugangsverlangens zu ermöglichen, um diesen nicht unangemessen zu belasten.

o) Hinsichtlich der Beweislastverteilung ist festzustellen, dass diese im Wesentlichen den allgemeinen Grundsätzen der Darlegungs- und Beweislast folgt.

p) Die Rechtsdurchsetzung ist abhängig von der Eröffnung des Rechtsweges. Ob der Zivilrechtsweg oder der Verwaltungsrechtsweg eröffnet ist, beurteilt sich nach allgemeinen Grundsätzen. Besonderheiten ergeben sich allein, wenn der Zugangsverpflichtete zwar eine Privatperson ist, Datenzugang aber nur durch eine Dritte Instanz, z.B. den Koordinator für digitale Dienste begehrt werden kann. Bleibt dieser untätig, so ist er auf dem Verwaltungsrechtsweg zum Tätigwerden gegen den privaten Zugangsadressaten zu verpflichten. Der Verwaltungsrechtsweg ist immer dann eröffnet, wenn entweder eine aufdrängende Sonderzuweisung diese Rechtsfolge vorsieht oder aber wenn die Voraussetzungen der Generalklausel des § 40 Abs. 1 S. 1 Hs. 1 VwGO erfüllt sind und die Streitigkeit nicht im Wege einer abdrängenden Sonderzuweisung ausdrücklich einer anderen Gerichtsbarkeit zugewiesen wird.

16. Hinsichtlich der Gewährung von Forschungsdatenzugang in den Rechtsordnungen der Staaten Indien, Frankreich, Kanada, Finnland, Australien und Großbritannien im Gesundheitssektor ist festzuhalten:

a) Der vorgeschlagene Regulierungsrahmen für nicht-personenbezogene Daten in Indien ist hoch innovativ, verfolgt aber ausweislich der im Expertenreport benannten Beispiele v.a. den Zweck, Datenzugang zugunsten des Staates im Gemeinwohlinteresse zu sichern. Datenzugang für Wissenschaft und Forschung kann und sollte sich nicht allein auf Daten beziehen, die von einer i.d.R. behördlichen Instanz als im öffentlichen Interesse liegende Daten im Sinne eines High-value Datasets (HVD) erklärt werden. Forschung und Wissenschaft benötigt vielmehr Zugang zu nicht vordefinierten Daten. Ob die Forschung selbst dann im öffentlichen Interesse liegen muss, ist eine davon zu unterscheidende Frage. Eine zentrale Zwischeninstanz, die Forschern als Ansprechpartner dient und ihnen den Zugang zu von Dritten erhobenen Daten mittelt, kann den Datenzugangsprozess für Forschung und Wissenschaft erleichtern. Nicht zwingend ist aber, dass die Daten auch zentral bei dieser Stelle liegen. Vielmehr könnte die Instanz den Zugang auch zu dezentral bei den Unternehmen selbst liegenden Daten mitteln und diese damit von der zeit- und ressourcenbelastenden Aufgabe des Datenzugangs entlasten.

Wesentlich für den Forschungsdatenzugang in Indien aber ist nicht nur die effektive Zwischenschaltung einer Datenmittelungsinstanz, sondern auch die Tatsache, dass Adressaten des

Datenzugangsanspruchs private Stellen sein können und dass der Datenzugangsanspruch sektorübergreifend und damit als horizontale Regelung ausgestaltet ist.

b) In Frankreich wurde 2018 eine Expertenkommission eingerichtet, die die Einrichtung eines Datenraumes empfahl, der von möglichst vielen Parteien genutzt werden kann und diesen zugänglich ist.

Im Dezember 2019 wurde eine erste Version dieses Health Data Hubs vorgestellt, im April 2020 wurde sie in den Echtzeitbetrieb genommen. Eingespeist werden Daten des nationalen Gesundheitsdatensystems. Hierzu gehören beispielsweise Krankenversicherungsdaten, Daten von Vorsorgeuntersuchungen, Daten von Mütter- und Kinderschutzdiensten etc. Es handelt sich also um eine Zusammenfassung staatlich erhobener Gesundheitsdaten bei einer Zentralverwaltungsinstanz. Über den Zugang zu den Daten entscheidet ein Ethics Committee, das mit dem „Arrêté du 26 mai 2020 portant nomination des membres du Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé“ eingerichtet wurde. Es prüft, ob das Forschungsprojekt einen Beitrag zum öffentlichen Interesse leistet. Die Nutzung der Daten zu kommerziellen Werbezwecken ist untersagt, die Daten dürfen nicht verkauft werden.[15] Der Datenzugang zu personenbezogenen Daten im nationalen Gesundheitsdatensystem darf nach L 1461-3 Code de la Santé Publique nur für Zwecke nach L-1461-1 genehmigt werden. Zu diesen Zwecken gehören nach L 1461-1 Abs. 2 Nr. 2 die Zwecke von Forschung, Studien, Evaluationen und Innovation in den Bereichen Gesundheit und medizinisch-soziale Versorgung. Es handelt sich dem Wortlaut des L 1461-1 und L1461-3 nach um eine echte Forschungsklausel im Sinne eines Datenzugangsanspruchs. Der Zugang zu den in 1461-2 Code de la Santé Publique benannten Daten erfolgt bislang kostenlos. Auch der Zugang zu anderen als den in Artikel L. 1461-2 genannten Gesundheitsdaten ist kostenlos zumindest für Forschung, die ausschließlich für den Bedarf der öffentlichen Verwaltung durchgeführt wird. Die Erarbeitung von Geschäftsmodellen und Finanzierungsmöglichkeiten für den Zugang zu Daten des Health Data Hubs ist aber Gegenstand eines weiteren Reflektionsprozesses bis 2022. Seit dem 21. April erlaubt ein Ministerialerlass dem Hub, eine Vielzahl von Gesundheitsdaten für die Zwecke der Forschung im öffentlichen Interesse zu erhalten[16] und in der Folge auch bereitzustellen.

c) In Kanada existiert eine Vielzahl von Regelungen, die es staatlichen Stellen gestatten, Datenzugang für wissenschaftliche Zwecke zu gewährleisten. Diese Datenzugangsansprüche scheinen sich aber

[15] *Stuwe*, Präsentation: Health Data Hub - Overview, strategy and lessons learned, 2020, abrufbar unter: http://ehaction.eu/wp-content/uploads/2020/10/D3S2_HDH-Louisa_Stuwe-new_version.pdf, zuletzt abgerufen am 16.07.2021.

[16] Arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire, abrufbar unter: https://www.legifrance.gouv.fr/download/file/JQCAhy2BjS_uSuRmKba4o_yPpUVXDsxSS7PEreByYJg=/JOE_TEXTE, zuletzt abgerufen am 16.07.2021.

sämtlich in der Erlaubnis der Datenzugangsgewährung zu erschöpfen und gerade keinen Anspruch auf Datenzugang zu gewährleisten.[17] Dies ergibt sich aus einer Wortlautanalyse der Vorschriften aus dem Gesundheitsbereich im Vergleich mit Vorschriften aus dem Verwaltungssektor, wo ein Datenzugangsanspruch ausweislich z.B. des „Art. Chapter IV Devision 2 125 des Act Respecting Access to Documents Held by Public Bodies and the Protection of personal Information"[18] durchaus existiert.[19]

Eine Übersicht dieser Erlaubnisse der Datenzugangsgewährung findet sich in einem Papier des "Expert Panels on Timely Access to Health and Social Data for Health Research and Health System Innovation". Auffällig ist, dass die Daten sämtlich „for approved data purposes" genutzt werden dürfen, wobei die Entscheidung über die Nutzung in der Regel von einer hierfür ausgewiesenen Stelle getroffen wird, z.B. von einem „Research Ethics Board" (REB). Außerdem sind Vereinbarungen über die Datennutzung zwischen dem Data Custodian (datenhaltende Stelle) und dem Forscher bzw. der Forschungseinrichtung zu schließen. Es existiert hier eine „Muster-Forschungsvereinbarung" des Ministeriums. Im Übrigen sind die Voraussetzungen des Datenzugangs höchst unterschiedlich. Die Antragsberechtigung ist allerdings i.d.R. auf spezifische Forscher innerhalb Kanadas beschränkt.

d) Echte Forschungsklauseln i.S.e. Datenzugangsanspruchs zugunsten von Forschung und Wissenschaft kennt das finnische Rechtssystem für den Gesundheitssektor insb. im Biobank-Act sowie im Act on Secondary Use of Health and Social Data (im Folgenden Secondary Use Act). Secondary Use meint dabei – im Gegensatz zum Primary Use – die Nutzung von Daten zu spezifischen anderen Zwecken als denjenigen, für die sie erhoben wurden, vgl. Art. 3 Act on the Secondary Use of Health and Social Data[20] Ein solcher privilegierter Zweck, für den ein Secondary Use möglich sein soll, ist die Forschung. Art. 38 des Secondary Use Act sieht zwar lediglich vor, *„a data permit may be granted"*, Abs. 2 enthält aber die Vorgabe, dass die Forschungsfreiheit bei der Erteilung der Erlaubnis berücksichtigt werden muss. Dies ließe sich für den Fall, dass einem Datenzugangsanspruch keine Rechte und Interessen des Zugangsverpflichteten oder Dritter entgegenstehen (z.B. Geheimnisschutzerwägungen) und datenschutzrechtliche Belange durch Schutzvorkehrungen ausreichend gewahrt werden, als Begründung eines Anspruchs auf Datenzugang verstehen. Erfasst sind Daten sowohl von öffentlichen Stellen, wie national data repositories, healthcare and social welfare care data archives, aber auch registrierte Daten privater Anbieter von Sozial- und Gesundheitsdienstleistungen. Datenzugang wird entweder gewährt durch die datenhaltende Instanz selbst (z.B. das Data Repository) oder durch eine

[17] Vgl. Office of the Information & Privacy Commissioner for British Columbia, Access to Data for Health Research, 2018, S. 10, abrufbar unter https://www.oipc.bc.ca/guidance-documents/2115, zuletzt abgerufen am 16.07.2021.
[18] Act respecting Access to Documents held by Public Bodies and the Protection of Personal Information, abrufbar unter http://legisquebec.gouv.qc.ca/en/pdf/cs/A-2.1.pdf, zuletzt abgerufen am 16.07.2021.
[19] Weitere Datenzugangsansprüche für den Verwaltungssektor finden sich im Access to Information Act sowie in Section 5 des Statistic Act i.V.m. Statistics Canada Policy on the Use of Administrative Data Obtained under the Statistics Act.
[20] *Lilja*, Secondary use of health data – the new Finnish Act, 2019, abrufbar under: https://www.roschier.com/newsroom/secondary-use-of-health-data-the-new-finnish-act/, zuletzt abgerufen am 16.07.2021.

neue Behörde, Findata (Data Permit Authority), die am Finnish Institute for Health and Welfare betrieben wird, von den übrigen Aktivitäten des Institutes allerdings unabhängig ist. Sie untersteht der Aufsicht des Ministry of Social Affairs. Wird eine Erlaubnis des Datenzugangs durch Findata erteilt, sammelt Findata die Daten von den datenhaltenden Instanzen, kombiniert und pseudonymisiert oder anonymisiert sie ggf. (als „Aufbereitung" der Daten bezeichnet) und stellt sie dem Antragsteller anschließend über einen spezifisch einzurichtenden sicheren Hosting-Service zur Verfügung. Wurden die Daten auf Grundlage einer datenschutzrechtlichen Einwilligung zur Verfügung gestellt, darf Datenzugang nur gewährt werden, wenn dies von der Reichweite der Einwilligung gedeckt ist.

e) In Australien ist der Zugang zu Forschungsdaten über den My Health Records Act gewährleistet. Das „My Health Record System" ist ein staatlich betriebenes System zur Bereitstellung von Gesundheitsinformationen über Gesundheitsversorgungsempfänger für die Zwecke der Gesundheitsversorgung des Empfängers (Primärnutzung) sowie für andere Zwecke, z.B. Zwecke von Wissenschaft und Forschung (Sekundärnutzung). Ein Gesundheitsversorgungsempfänger hat eine Gesundheitsakte in diesem System. Sobald er sich entweder registriert oder – für den Fall, dass ein Opt-Out-Modell vom Minister angeordnet wird – er nicht ausoptiert. Der Systembetreiber betreibt den National Repositories Service, der die wichtigsten Datensätze der Gesundheitsakte speichert. Andere Datensätze werden von registrierten Repository-Betreibern gespeichert. Zusammen bilden diese Datensätze die Persönliche Gesundheitsakte des Gesundheitsversorgungsempfängers. Erforderlich für den Datenzugang ist es, dass das „Data Governance Board", das mit verschiedenen Experten besetzt ist und von verschiedenen Gremien beraten wird, einen Auftrag auf Nutzung von Daten zu Forschungszwecken positiv bescheidet. Der Antragsteller muss zuvor den Nutzungsbedingungen zustimmen[21] und einen Risikomanagement-Plan beifügen, auf dessen Grundlage das Board insb. das Risiko eines Verlustes oder Missbrauchs der Daten beurteilt.[22] Für den Zugang zu personenbezogenen Daten ist außerdem stets die Einwilligung des Betroffenen erforderlich. Eine Datenweitergabe an Versicherer findet nicht statt. Das Board wendet bei der Bescheidung des Datenzugangsantrags das „Safe-People-Principle" an und bewertet bei der Zugangsentscheidung das Wissen, die Fähigkeiten und die Anreize des Antragstellers, Daten angemessen zu speichern und zu nutzen. Es handelt sich nicht um einen Ethikrat.

[21] *Australian Government - Department of Health*, Framework to guide the secondary use of My Health Record system data, 2018, S. 31, abrufbar unter: https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf, zuletzt abgerufen am 16.07.2021.

[22] *Australian Government - Department of Health*, Framework to guide the secondary use of My Health Record system data, 2018, S. 47, abrufbar unter: https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf, zuletzt abgerufen am 16.07.2021.

e) In Großbritannien existiert ein System von sieben Research Data Hubs,[23] die im Oktober 2019 von einer unabhängigen, eingetragenen Wohltätigkeitsorganisation, der „Health Data Research UK", eingerichtet wurden. Ein Anspruch auf Datenzugang existiert nicht, vielmehr entscheidet ein Gremium nach eigenen festgelegten Kriterien über die Datenzugangsgewährung. Werden personenbezogene Daten zur Verfügung gestellt, darf dies allein mit Einwilligung des Betroffenen erfolgen.[24] In dem Data Hub „Insight", die hier Vorbildcharakter hat, hat das zu diesem Zweck eingerichtete Data Trust Advisory Board (Data TAB) eine Reihe von Zugangskriterien entwickelt, die eine angemessene Prüfung ermöglichen und gleichzeitig praktikabel, effizient und skalierbar sind. Wer Zugang zu Daten erhalten soll und zu welchem Zweck, wird durch das sog. DataTAB entschieden.

17. Für den Mobilitätssektor existieren de lege lata keine umfassenden Vorbildregelungen. New South Wales, ein Bundesstaat in Australien, arbeitet mit einem Open Data Transport Hub, auf den jedermann nach vertragsrechtlichen Grundsätzen Zugriff nehmen kann, womit neue datengestützte Innovationen im Mobilitätssektor aber auch „policy research" ermöglicht werden soll.

18. Im Energiesektor ist der Forschungsdatenzugang ebenfalls unterentwickelt. Hier befindet sich in Großbritannien lediglich eine Plattform in der Entstehung, über die nach vertragsrechtlichen Grundsätzen Zugang zu Energiedaten gemittelt werden könnte. Welche Daten konkret betroffen sein könnten, ist aber noch nicht entschieden.

19. Im Online-Wirtschaftssektor existieren international keine Regelungen für den Forschungsdatenzugang. Hier können die nationalen Bestimmungen aber als Orientierungspunkt für eine rechts- und interessengerechte Ausgestaltung echter Forschungsklauseln dienen.

20. Datenzugangsansprüche sind zwingend gemeinsam mit Datenzugangsinfrastrukturen zu entwickeln, um eine hinreichende Effektivität der Ansprüche zu gewährleisten. Ein wichtiger Baustein in diesen Datenzugangsinfrastrukturen sind Forschungsdatenzentren und Datentreuhänder, zu denen auch Personal Information Management-Systeme (PIMS) zählen. Datenzugangsinfrastrukturen und Datenzugangsansprüche bilden ein Datenzugangsökosystem.

21. Aus der Analyse der nationalen und internationalen Forschungsklauseln lassen sich sektorspezifische Leitlinien für einen Forschungsdatenzugang entwickeln, die im Gesundheitsbereich in ein Gesamt-Forschungsdatenzugangsökosystem sowie ein Gesundheitsforschungsdatenzugangsgesetz übertragen werden können. Es empfiehlt sich für den

[23] Improving UK Health Data - Impacts from Health Data Research Hubs, 2021, abrufbar unter: https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs-v2.pdf, zuletzt abgerufen am 16.07.2021.
[24] Improving UK Health Data - Impacts from Health Data Research Hubs, 2021, abrufbar unter: https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs-v2.pdf, zuletzt abgerufen am 16.07.2021.

Gesundheitssektor ein gemischtes System originärer Forschungsklauseln mit zentralen Datenspeichern (z.B. bereits existenten Zentralregistern wie dem Bundeskrebsregister), dezentral-zentralen Datenspeichern (z.B. verteilten Registern wie den Landeskrebsregistern, wobei die Verteilung nicht zwingend auf Ebene der Bundesländer stattfinden muss) und gänzlich dezentralen Datenspeichern z.B. bei Gesundheitsdiensteanbietern. In dieses System zentraler, dezentral-zantraler und gänzlich dezentraler Datenspeicher könnten auch die Daten privater Gesundheitsdiensteanbieter eigespeist werden. Die Möglichkeit der Datenspende sollte auch und gerade über PIMS eröffnet werden. Auch die elektronische Patientenakte ließe sich als ein derartiges PIMS verstehen. Bei der regulatorischen Ausgestaltung von Datenzugangsansprüchen sollte in der Regel eine enge Zweckbindung an gemeinwohlorientierte Forschung normiert werden. Ist dies der Fall, muss der Kreis der Datenzugangsberechtigten nicht auf die nicht-kommerzielle Forschung beschränkt werden. Versicherungen sollten von der Anspruchsberechtigung ausgeschlossen werden. Ein Erforderlichkeitskriterium des Datenzugangs ist nicht vorzusehen. Im Interesse des Schutzes konfligierender Rechte und Interessen sollte aber ein Schutzkonzept verlangt werden, und zwar unabhängig davon, ob die Daten anonymisiert oder personenbezogen übermittelt werden. Für den Datenzugangsantrag sollte im Interesse einer effektiven Gewährleistung des Datenzugangs ein standardisiertes - idealerweise international einheitliches - Verfahren vorgesehen werden. Es empfiehlt sich außerdem die in einigen ausländischen Rechtsordnungen (Frankreich, Kanada, Finnland, Australien) vorgesehene Einbindung einer Instanz, die über die ethische Vereinbarkeit der Forschung entscheidet. Zusätzliche Antragsvoraussetzung sollte die positive Prüfung durch dieses Research Ethics Board (REB) sein. In Kanada entscheidet diese Instanz auch und gerade darüber, ob die Daten „for approved data purposes“ genutzt werden. Diese Funktion wird in Australien von dem Data Governance Board vorgenommen. Hier scheint eine Trennung zwischen beiden Instanzen sinnvoll, denn die Entscheidung über die ethische Vereinbarkeit des Forschungsvorhabens sollte primär durch Ethiker getroffen werden, während die Prüfung, ob die Forschung den vorausgesetzten Gemeinwohlinteressen dient und auch im Übrigen die materiell-rechtlichen Voraussetzungen des Datenzugangsanspruchs erfüllt sind, eine juristische Frage ist. Die Anschlussnutzung der Daten sollte klar definiert werden. Sie sind frühestmöglich zu pseudonymisieren, zu anonymisieren oder zu löschen. Eine Nutzung der Daten zu kommerziellen Werbezwecken sollte ebenso untersagt werden, wie ein Verkauf der Daten. Auch eine gänzliche Untersagung der Datenweitergabe ist denkbar. Dies würde das Risiko einer missbräuchlichen Verwendung senken, weshalb der Datenzugangsanspruch zugunsten von Forschung und Wissenschaft im Gegenzug nach dem Five Safes Model weitreichender ausfallen dürfte als im Falle der Zulässigkeit einer Forschungsdatenweitergabe. Anonymisierte Daten sollten nicht de-anonymisiert werden dürfen, wobei das Verbot der De-Anonymisierung auch strafrechtlich

adressiert werden sollte.[25] Gleichzeitig sind im Interesse von Rechtsklarheit und zur Wahrung des Bestimmtheitsgebotes Standards zur Anonymisierung vorzusehen. Der Datenzugang darf die Rechte und Interessen Dritter nicht über Gebühr einschränken. Dies ist als Schrankenbestimmung nach dem Vorbild von Art. 15 DSGVO vorzusehen. Vergütungsregelungen sollten sich auf eine Kostendeckung der Verwaltungstätigkeit beschränken. Orientiert werden sollte sich an der Datentransparenz-Gebührenverordnung. Fristenregelungen im Verwaltungsbereich sollten stets einhergehen mit einer ausreichenden Personal- und Sachmitteldeckung. Gleichzeitig muss eine sorgfältige Prüfung des Datenzugangs gewährleistet sein. Flexible Fristenregelungen mit einer Obergrenze sind daher starren Fristenregelungen, die nicht oder nur unzureichend auf den konkreten Bearbeitungsaufwand reagieren können, vorzuziehen. Eine Orientierung an Finnlands Secondary Use Act die Entscheidung über einen data-permit unverzüglich zu treffen, spätestens aber 3 Monate nach Eingang des vollständigen Antrags bei der Behörde, ist zu empfehlen. Entscheidungen über den Datenzugang ergehen in der Form des Verwaltungsaktes. Der statthafte Rechtsweg für den Fall eines ablehnenden Bescheides ist daher die Verpflichtungsklage gerichtet auf den Erlass eines stattgebenden Verwaltungsaktes. Es gelten grundsätzlich die allgemeinen Beweislastregelungen. Das Gemeinwohlinteresse sollte aber, wenn die Forschung an öffentlichen Forschungseinrichtungen erbracht und die Forschungsergebnisse (anonymisiert) der Öffentlichkeit zugänglich gemacht werden, vermutet werden. Neben einem System zentraler, dezentral-zentraler und gänzlich dezentraler Speicher von Forschungsdaten sollten flexible Datentreuhandstrukturen vorgesehen und auf eine rechtssichere Grundlage gestellt werden.

22. Für den Online-Wirtschaftssektor lässt sich aus der Analyse der nationalen und internationalen Forschungsklauseln eine Musterforschungsdatenzugangsklausel ableiten, die in einer Reihe identifizierter Gesetze als abgeleitete und originäre Forschungsklauseln normiert werden sollte. Auch im Online-Wirtschaftssektor sollte Zugang zu den Daten privater und öffentlicher Stellen durch mittelbare Datenzugangsstrukturen in staatlicher Organisation gewährleistet werden. D.h. konkret, dass entsprechend Art. 31 DSE-E der Koordinator für Digitale Dienste oder eine ähnliche Instanz über den Datenzugang entscheiden sollte, um die privaten Stellen von der Datenzugangsentscheidung zu entlasten. Eine Beschränkung des Datenzugangsanspruchs auf spezifische Forschungsvorhaben muss nicht stattfinden. Wird eine solche Beschränkung nicht vorgenommen, empfiehlt sich aber eine asymmetrische Regulierung, d.h. eine Adressierung von Unternehmen der Privatwirtschaft erst ab einer gewissen Größe, die eine wirtschaftliche Überforderung durch die Verpflichtung zum Datenzugang ausschließt. Im Übrigen kann sich im Wesentlichen an den

[25] *Specht*, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, 1040, 1046-1047; Gutachten der Datenethikkommission, 2019, S. 132, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 16.07.2021.

Datenzugangsvoraussetzungen im Gesundheitssektor orientiert werden. Anders als im Gesundheitssektor sind im Online-Wirtschaftssektor aber private Stellen im Falle eines berechtigten Datenzugangsanspruches verpflichtet, die Daten bereit zu stellen. Dies kann mit einem erheblichen Aufwand verbunden sein, der zu entschädigen ist. Gleichzeitig kann eine überhöhte Vergütung die Effektivität des Datenzugangsanspruchs erheblich beeinträchtigen. § 5a NetzDG geht daher den Weg einer Höchstgrenze von 5.000 EUR und stellt die Angemessenheit der Höhe im Übrigen in das Ermessen des Gerichts nach § 287 ZPO. Dies scheint der einzig gangbare Weg, wobei die konkrete Bezifferung der Höchstgrenze je Anfrage zu bestimmen und bestenfalls evidenzbasiert festgelegt werden sollte. Gegen die Entscheidung des Koordinators für digitale Dienste müssen sowohl die Forscher als auch die Zugangsverpflichteten vorgehen können. Für den Fall der Versagung der Datenzugangsgewährung von Seiten des Zugangsverpflichteten sollte der Anspruchsberechtigte den Anspruchsverpflichteten direkt in Anspruch nehmen können, ohne ein weiteres Tätigwerden des Koordinators für digitale Dienste abwarten zu müssen. Versagt der Koordinator für digitale Dienste dem Anspruchsberechtigten den Anspruch, so kann der Anspruchsberechtigte im Wege der Verpflichtungsklage gegen diesen vorgehen.

23. Im Mobilitätssektor und im Energiesektor sollte mangels nationaler und internationaler Best-Practice-Regelungen zunächst nach dem Vorbild Großbritanniens eine Expertenkommission eingesetzt werden, die Empfehlungen insb. für die von einem Datenzugangsanspruch erfassten Daten und die passende Datenzugangsinfrastruktur entwickeln wird. Im Mobilitätssektor sollten dabei die bereits von verschiedenen Stellen verfolgten Ansätze von Mobilitätsdatenräumen und -plattformen zusammen gedacht werden.

IV. Prinzipien eines Forschungsdatenzugangsregimes

1. Openness by Design

Die Offenlegung von Daten ist nicht nur ein Treiber für Innovation, auch die Forschung würde erheblich von einem offenen Datenzugang profitieren. Im gesamtgesellschaftlichen Interesse sollten Daten daher als Default-Einstellung offenzulegen sein („openness by design“). Dies gilt zuvorderst für Verwaltungsdaten. Offenheit von Daten kann aber in verschiedenen Graden erreicht werden, die sich wie folgt beschreiben lassen:[26]

1. Offen (open data): Daten werden für alle zur Nutzung, Änderung und Verteilung ohne Einschränkungen zur Verfügung gestellt

2. Öffentlich (public data): Daten werden öffentlich zugänglich gemacht, aber mit einigen Nutzungseinschränkungen

3. Gemeinsam genutzt (shared data): Daten werden einer begrenzten Gruppe von Teilnehmern zur Verfügung gestellt, möglicherweise mit einigen Nutzungseinschränkungen

4. Geschlossen (closed data): Die Daten sind nur innerhalb einer einzigen Organisation verfügbar

Der Grad der möglichen Offenheit ergibt sich im Wesentlichen aus dem Risiko für die Rechte und Interessen der von der Datenverarbeitung Betroffenen. Sowohl bei der Offenlegung von Verwaltungsdaten als auch bei der Offenlegung privater Daten können datenschutzrechtliche Belange berührt werden. Diesem Risiko kann allerdings häufig angemessen durch Anonymisierung oder Pseudonymisierung begegnet werden. Erst wenn dies nicht möglich ist, ist es erforderlich, die Offenlegung von Daten zu beschränken oder den Zugang zu begrenzen.[27] Der Geschäftsgeheimnisschutz wird hingegen wesentlich häufiger berührt sein im Falle des Zugangs zu privat gehaltenen Daten als im Falle von Verwaltungsdaten. Daher ist es sinnhaft, die Default-Einstellung für Verwaltungsdaten insgesamt von „geschlossen“ zu „offen“ oder „öffentlich“ zu ändern, während die Default-Einstellung für privat gehaltene Daten von „geschlossen“ zu „gemeinsam genutzt“ geändert werden sollte. Dies muss jedenfalls für spezifische Zwecke gelten, die das Interesse an einer exklusiven Haltung der Daten überwiegen. Als solches Interesse kommt insb. die Forschung im Gemeinwohlinteresse in Betracht (dazu sogleich).

[26] A strategy for a Modern Digitalised Energy System - Energy Data Taskforce report, 2019, S. 25, abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/Catapult-Energy-Data-Taskforce-Report-A4-v4AW-Digital.pdf, zuletzt abgerufen am 16.07.2021.
[27] A strategy for a Modern Digitalised Energy System - Energy Data Taskforce report, 2019, S. 25, abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/Catapult-Energy-Data-Taskforce-Report-A4-v4AW-Digital.pdf, zuletzt abgerufen am 16.07.2021.

2. Five Safes Model

Für die Maßstäbe eines Datenzugangs wurde das sogenannte „Five Safes Model“ entwickelt, das den Datenzugang als ein Spektrum von fünf Risikodimensionen sieht. Jede dieser Dimensionen ruft eine spezifische Frage für den Datenzugang hervor, die bestenfalls regulatorisch zu beantworten ist:[28]

Abb. 1: Desai/Ritchie/Welpton, Five Safes: Designing data access for research, Economics Working Paper Series 1601, 2016, S. 5

Safe projects	Is this use of the data appropriate?
Safe people	Can the researchers be trusted to use it in an appropriate manner?
Safe data	Is there a disclosure risk in the data itself?
Safe settings	Does the access facility limit unauthorised use?
Safe outputs	Are the statistical results non-disclosive?

Das Five Safes Model beschreibt , wie Daten geschützt und das Risiko verringert werden kann, dass zu Unrecht auf Daten zugegriffen wird oder sie unsachgemäß verwendet werden. Auch der „UK Data Service“[29] und das Data Innovation Program in British Columbia[30] arbeiten mit den Five Safes.[31] Die Risikodimensionen beeinflussen sich dabei gegenseitig: Je stärker sichergestellt, dass die Daten innerhalb „sicherer Projekte“ verwendet werden, z.B. für Projekte im Gemeinwohlinteresse, und je stärker ebenfalls sichergestellt ist, dass nur bestimmte Personen Zugriff haben, desto weitgehender können auch risikobehaftete Daten, z.B. mit Personenbezug, zugänglich gemacht werden.[32] Diesem Ansatz folgen auch die hier entwickelten Datenzugangsgesetze.

Weiterhin ist dem bekannten Phänomen zu begegnen, dass eine weitgehende Beschränkung der Datennutzung in der Regel zu einer weitergehenden Umgehung dieser Nutzungsbeschränkung führt und dass Strafen hieran wenig ändern. Die Möglichkeit eines Ausschlusses vom Datenzugang wird dagegen eher ernst genommen. [33] Auch dieser Umstand wird im Rahmen dieser Untersuchung aufgegriffen.

3. FAIR Data Principles

[28] *Desai*/*Ritchie*/*Welpton*, Five Safes: Designing data access for research, Economics Working Paper Series 1601, 2016, S. 5, abrufbar unter: https://www2.uwe.ac.uk/faculties/bbs/Documents/1601.pdf, zuletzt abgerufen am 16.07.2021.
[29] https://www.ukdataservice.ac.uk/manage-data/legal-ethical/access-control/five-safes, zuletzt abgerufen am 16.07.2021.
[30] https://www2.gov.bc.ca/gov/content/data/about-data-management/data-innovation-program/privacy-security, zuletzt abgerufen am 16.07.2021.
[31] Für weitere Beispiele vgl. *Desai*/*Ritchie*/*Welpton*, Five Safes: Designing data access for research, Economics Working Paper Series 1601, 2016, S. 16, abrufbar unter: https://www2.uwe.ac.uk/faculties/bbs/Documents/1601.pdf, zuletzt abgerufen am 16.07.2021.
[32] https://www.ukdataservice.ac.uk/manage-data/legal-ethical/access-control/five-safes, zuletzt abgerufen am 16.07.2021.
[33] *Desai*/*Ritchie*/*Welpton*, Five Safes: Designing data access for research, Economics Working Paper Series 1601, 2016, S. 9, abrufbar unter: https://www2.uwe.ac.uk/faculties/bbs/Documents/1601.pdf, zuletzt abgerufen am 16.07.2021.

Darüber hinaus sollte sich Datenzugang für Wissenschaft und Forschung von den 2014 im Rahmen eines Workshops in Leiden für das Forschungsdatenmanagement entwickelten und zwischenzeitlich durch eine Arbeitsgruppe fortgeschriebenen FAIR-Prinzipien orientieren.[34] Diese Prinzipien sollen eine bessere und leichtere Verwendbarkeit von Forschungsdaten ermöglichen. Daten müssen danach zunächst auffindbar („findable“) sein. Dafür könnte ihnen und den dazugehörigen Metadaten z.B. eine weltweit einzigartige, dauerhafte Kennzeichnung gegeben werden. Die Daten müssten zudem umfangreiche deskriptive Metadaten erhalten, die auch die beschriebene Kennzeichnung enthielten. Zuletzt müssten die Daten wie die Metadaten in einer durchsuchbaren Datenbank o.ä. enthalten sein. Außerdem sollten die Daten zugänglich („accessible“) sein. Dafür könnten sie sowie die dazugehörigen Metadaten anhand ihrer Kennzeichnung beispielsweise mittels eines standardisierten Kommunikationsprotokolls abrufbar sein. Dieses Protokoll sollte die Implementierung von Authentifizierungs- sowie Autorisierungsprozessen erlauben. Zusätzlich müssten die Daten interoperabel („interoperable“) sein. Zu diesem Zweck müssten sie und die dazugehörigen Metadaten eine formale, zugängliche, gemeinsame und weit anwendbare Sprache der Wissensdarstellung nutzen. Zudem müssten sie qualifizierte Verweise auf andere Daten bzw. Metadaten enthalten. Erforderlich sind auch Systeme, die den Datenaustausch zulassen und idealerweise fördern, v.a. durch entsprechende Schnittstellen und Datenformate. Zuletzt müssen die Daten wiederverwendbar („reusable“) sein. Dies lässt sich v.a. durch entsprechende Beschreibung und transparente Zugangsbedingungen gewährleisten.[35]

[34] *Wilkinson* et al., Comment: The FAIR Guiding Principles for scientific data management and stewardship, Nature - Scientific Data, 2016, S. 3, abrufbar unter: https://www.nature.com/articles/sdata201618.pdf, zuletzt abgerufen am 16.07.2021; zu den FAIR Data Principles im Kontext von Datensouveränitätserwägungen vgl. *Hummel*/*Braun*/*Augsberg*/*von Ulmenstein*/*Dabrock*, Datensouveränität - Governance-Ansätze für den Gesundheitsbereich, 2021, S. 29, abrufbar unter: https://link.springer.com/content/pdf/10.1007%2F978-3-658-33755-1.pdf, zuletzt abgerufen am 16.07.2021.

[35] *Wilkinson* et al., Comment: The FAIR Guiding Principles for scientific data management and stewardship, Nature - Scientific Data, 2016, S. 3, abrufbar unter: https://www.nature.com/articles/sdata201618.pdf, zuletzt abgerufen am 16.07.2021; *Lehne*/*Sass*/*Essenwanger*/*Schepers*/*Thus*, Why digital medicine depends on interoperability, npj Digital Medicine, 2019, abrufbar unter: https://www.nature.com/articles/s41746-019-0158-1.pdf, zuletzt abgerufen am 16.07.2021; *Hummel*/*Braun*/*Augsberg*/*von Ulmenstein*/*Dabrock*, Datensouveränität - Governance-Ansätze für den Gesundheitsbereich, 2021, S. 29, abrufbar unter: https://link.springer.com/content/pdf/10.1007%2F978-3-658-33755-1.pdf, zuletzt abgerufen am 16.07.2021.

V. (Unions-)Grundrechtlicher und Kompetenzrechtlicher Rahmen eines Forschungsdatenzugangsregimes

1. (Unions-)Grundrechtlicher Rahmen

a) Datenzugangsbedingte Grundrechtskollisionen

Je nachdem, auf welcher Ebene Datenzugangsansprüche eingeführt werden, richtet sich der Rahmen für die Gewährung derartiger Datenzugangsansprüche nach den nationalen Grundrechten oder aber nach GRCh und EMRK. Dabei sind jeweils die Rechtspositionen des Datenzugangsadressaten, die Grundrechte Drittbetroffener sowie die grundrechtlichen Interessen der Zugangssuchenden in einen angemessenen Ausgleich zu bringen. Auf Seiten des Datenzugangsadressaten sind v.a. der – je nach vertretener Auffassung[36] – in Art. 12 respektive Art. 14 GG sowie – wiederum je nach vertretener Ansicht[37] – in Art. 17 GRCh bzw. Art. 6, 15, 16 GRCh verankerte Geschäftsgeheimnisschutz berührt, ebenso sind aber der in Art. 14 GG und Art. 17 GRCh normierte Schutz des Geistigen Eigentums, z.B. der urheberrechtliche Datenbankschutz nach § 2 UrhG aber auch das sui generis Recht des § 87a UrhG[38] sowie der Schutz der Berufsfreiheit (Art. 12 Abs. 1 GG bzw. Art. 15 Abs. 1 GRCh) zu berücksichtigen. Auf Seiten der von einem Datenzugang Drittbetroffenen ist v.a. das informationelle Selbstbestimmungsrecht, Art. 2 Abs. 1, 1 Abs. 1 GG bzw. Art. 7 und 8 GRCh zu beachten und auf Seiten der Zugangssuchenden die Freiheit von Forschung und Wissenschaft gem. Art. 5 Abs. 3 GG bzw. Art. 13 GRCh.

Der Eingriff in die Rechtspositionen der Datenzugangsadressaten verfolgt mit der Gewährung der Tätigkeit von Forschung und Wissenschaft einen legitimen Zweck, im Rahmen der Geeignetheit hat der Gesetzgeber traditionell einen sehr weiten Einschätzungsspielraum,[39] der im Falle einer Gewährung des Datenzugangs zugunsten von Forschung und Wissenschaft nicht überschritten sein dürfte. Freiwillige Maßnahmen als milderes Mittel im Rahmen der Erforderlichkeit dürften jedenfalls nicht gleich geeignet sein. Im Rahmen der Angemessenheit dürfte sich ein Datenzugang im

---

[36] Vgl. BVerfGE 115, 205 (229) = NVwZ 2006, 1041; BVerfGE 128, 1 (56) = NVwZ 2011, 94 = NJW 2011, 441 Ls.; BVerfGE 137, 185 (255 f.) = NVwZ 2014, 1652.

[37] *Wollenschläger*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Art. 17 GRC Rn. 16; *Wollenschläger*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Art. 16 GRC Rn. 8; *Aplin*, Right to Property and Trade Secrets, in: Geiger, Research Handbook on Human Rights and Intellectual Property, 2015, S. 421-437; *Breuer*, Staatliche Berufsregelung und Wirtschaftslenkung, in Isensee/Kirchhof, Handbuch des Staatsrechts: Band VIII, Grundrechte: Wirtschaft, Verfahren, Gleichheit, 3. Auflage, 2010, § 171 Rn. 38.

[38] *Wischmeyer*/*Herzog*, Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, NJW 2020, 288, 290: „*Insoweit sprechen gute Gründe dafür, die Position des Datenbankherstellers als Eigentum i.S.d. Art. 14 anzuerkennen.*"; *Fechner*, Geistiges Eigentum und Verfassung, 1999, S. 371.

[39] Explizit für Fälle der Datenzugangsgewährung: *Wischmeyer*/*Herzog*, Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, NJW 2020, 288, 293.

Gemeinwohlinteresse sehr viel eher rechtfertigen lassen als ein Datenzugangsanspruch im Privatinteresse, weil die Gemeinwohlinteressen i.d.R. wesentlich schwerer wiegen sollten. Auch entsprechende Kompensationsmöglichkeiten des Datenzugangsadressaten dürften zu einer Angemessenheit der Regelung beitragen.[40]

b) (Unions-)Grundrechtliche Gewährleistungen der Forschungsfreiheit

Innerhalb dieser Grundrechtskollisionen kommt der Forschungsfreiheit im hier relevanten Kontext erhebliche Bedeutung zu. Zu ihren Gunsten soll der Datenzugang gewährleistet werden, weshalb im Folgenden v.a. ihr sachlicher Schutzbereich in Art. 13 GRCh und Art. 5 Abs. 3 GG der Erläuterung bedarf.

Die Mitgliedstaaten sind an die Gemeinschaftsgrundrechte gebunden, wenn sie Gemeinschaftsrecht in nationales Recht umsetzen, Gemeinschaftsrecht vollziehen oder die Grundfreiheiten innerstaatlich beschränken.[41] Wo die Mitgliedstaaten aber kein Gemeinschaftsrecht vollziehen, gilt das grundgesetzliche Begriffsverständnis der Forschungsfreiheit. Beide Begriffsverständnisse decken sich aber weitgehend: Nach Art. 13 GRCh sind Kunst und Forschung frei. Die akademische Freiheit wird geachtet. Der EuGH hat den Begriff der Forschung bislang nicht definiert, die Literatur greift aber auf die Rechtsprechung des BVerfG zurück, da Art. 13 GRCh als vom deutschen Grundgesetz inspiriert gilt.[42] Das Bundesverfassungsgericht definiert Wissenschaft als „jede Tätigkeit, die nach Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist".[43] Wissenschaftliche Forschung ist laut Bundesverfassungsgericht die „geistige Tätigkeit mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen".[44] Es wird ein besonderes methodisches Vorgehen und ein bestimmter Kenntnisstand verlangt.[45] Unerheblich ist dagegen, ob die Forschung innerhalb oder außerhalb von Hochschulen stattfindet.[46] Der Begriff der Forschung ist weit zu verstehen und umfasst auch die private Forschung.[47] Geschützt werden selbst

[40] In diesem Sinne wohl auch: *Wischmeyer*/*Herzog*, Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, NJW 2020, 288, 293.
[41] *Ehlers*, in: Ehlers, Europäische Grundrechte und Grundfreiheiten, 3. Auflage, 2009, § 14 Rn. 50; *Wissenschaftliche Dienste des Deutschen Bundestages*, Die Wissenschaftsfreiheit im Grundgesetz und in der Charta der Grundrechte der Europäischen Union, Ausarbeitung, S. 5, abrufbar unter: https://www.bundestag.de/resource/blob/420386/07891b8c2e2b3a104b0ffd0128619ba1/WD-3-149-10-pdf-data.pdf, zuletzt abgerufen am 16.07.2021.
[42] *Schlösser-Rost*/*Koch,* in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, BDSG § 27 Rn. 15a-20.
[43] BVerfGE 47, 327 (367); BVerfGE 35, 79 (113); siehe auch *Jarass*, in: Jarass, EU-Grundrechte-Charta, 4. Auflage, 2021, Art. 13 Rn. 8 mwN.
[44] BVerfGE 35, 79 (113).
[45] *Pernice*, in: Dreier, Grundgesetz-Kommentar, 2. Auflage, 2004, Art. 5 III Rn. 27; *Wissenschaftliche Dienste des Deutschen Bundestages*, Die Wissenschaftsfreiheit im Grundgesetz und in der Charta der Grundrechte der Europäischen Union, Ausarbeitung, S. 5, abrufbar unter: https://www.bundestag.de/resource/blob/420386/07891b8c2e2b3a104b0ffd0128619ba1/WD-3-149-10-pdf-data.pdf, zuletzt abgerufen am 16.07.2021.
[46] *Jarass*, in: Jarass, EU-Grundrechte-Charta, 4. Auflage, 2021, Art. 13 Rn. 8 mwN; *Bernsdorff*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage, 2019, Art. 13 Rn. 14.
[47] *Bernsdorff*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage, 2019, Art. 13 Rn. 14.

vorbereitende und unterstützende Aktivitäten.[48] Grundrechtsträger sind neben natürlichen und juristischen Personen (sofern Art. 5 Abs. 3 GG seinem Wesen nach auf diese juristischen Personen anwendbar ist, Art. 19 Abs. 3 GG) auch Hochschulen, selbst wenn sie Anstalten oder Körperschaften des öffentlichen Rechts sind.[49]

2. Kompetenzrechtlicher Rahmen

a) Gesetzgebungskompetenz

Der Digital Services Act, in dem auch eine Forschungsklausel vorgesehen ist, beruht auf der Binnenmarktkompetenz in Art. 114 AEUV, ebenso wie der Data Act, der weitergehende Datenzugangsbefugnisse regeln soll. V.a. Datenzugangsansprüche, die auch gegen Private gerichtet sind, sollten zwecks Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben, damit auf dieser Grundlage erlassen werden können. Selbst die PSI-RL wurde auf Grundlage der Binnenmarktkompetenz erlassen, obwohl sie lediglich den Zugang zu Verwaltungsdaten regelt. Auch Datenzugang gegen staatliche Akteure wird also auf diese Kompetenz gestützt. Art. 114 AEUV schafft allerdings keine ausschließliche Kompetenz des europäischen Gesetzgebers. Hat der Gemeinschaftsgesetzgeber keine abschließende Harmonisierung vorgenommen, können die Mitgliedstaaten auch weiterhin in eigener Zuständigkeit nationale Vorschriften auf dem betreffenden Sachgebiet erlassen.[50]

Im nationalen Recht sind grundsätzlich die Länder für Forschungsgesetzgebung zuständig, wenn nicht eine Bundeskompetenz explizit etwas anderes vorsieht. Eine konkurrierende Gesetzgebungskompetenz des Bundes gemäß Art. 74 Abs. 1 Nr. 13 i.V.m. Art. 72 Abs. 2 GG ist allerdings auf dem Gebiet der Förderung der wissenschaftlichen Forschung vorgesehen. Datenverarbeitungen, die im Sachzusammenhang mit der Forschung stehen, können daher bundeseinheitlich geregelt werden.[51] Der Begriff der Forschungsförderung umfasst neben finanziellen Fördermaßnahmen auch organisatorische und planerische Maßnahmen zur Förderung von Forschungsprojekten und Forschungseinrichtungen.[52] Auch wenn die Kompetenzklausel unscharf formuliert ist, bisher kaum auf sie zurückgegriffen wird und ein Rückgriff daher notwendigerweise Rechtsunsicherheit mit sich bringt,

---

[48] *Jarass*, in: Jarass, EU-Grundrechte-Charta, 4. Auflage, 2021, Art. 13 Rn. 8; *Bernsdorff*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage, 2019, Art. 13 Rn. 14.

[49] *Starck*, in: v. Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, 5.Auflage, 2005, Art. 5 III Rn. 408; *Kempen*, in: Epping/Hillgruber, BeckOK Grundgesetz, 47. Edition, 2021, Art. 5 Rn. 179-182.

[50] *Grussmann*/*Honekamp*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, 4. Auflage, 2013, B. Europarechtliche Grundlagen, Rn. 84.

[51] *Dierks*, Rechtsgutachten Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, S. 31, abrufbar unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/RECHTSGUTACHTEN_Gesundheitsforschungsdatenschutzrecht_BMG.pdf, zuletzt abgerufen am 16.07.2021.

[52] *Seiler*, in: Epping/Hillgruber, BeckOK Grundgesetz, 41. Edition, 2019, Art. 74 Rn. 54.

so lässt sich doch sagen, dass zumindest eine scharfe Begrenzung auf die finanzielle Förderung nicht vorgesehen ist, lediglich Auswirkungen der Bundesgesetzgebung auf die Hochschulstrukturen sollten ausgeschlossen werden. Auf eine Gesetzgebung zwecks Beseitigung nichtfinanzieller und systemischer Forschungshemmnisse ließe sich Art. 74 Abs. 1 Nr. 13 daher durchaus erstrecken.[53]

Im Rahmen der Datenverarbeitungsbefugnisse müssen freilich die Vorgaben und Sperrwirkungen der DSGVO beachtet werden, d.h. datenschutzrechtliche Abweichungen von den Vorgaben der DSGVO sind nur möglich zur Ausfüllung einer etwaigen Öffnungsklausel.

b) Achtung des Herkunftslandprinzips bei Normierung von Forschungsklauseln im Online-Wirtschaftssektor

Werden Diensteanbieter mit Sitz außerhalb der EU vom Forschungsdatenzugang adressiert, wie dies insb. im Online-Wirtschaftssektor der Fall sein dürfte, stellt sich die Frage, ob dies gegen das Herkunftslandprinzip der E-Commerce-Richtlinie (ECRL) verstößt. Das Herkunftslandprinzip ist in Art. 3 ECRL normiert, der die Primärverantwortlichkeit des Mitgliedstaates vorschreibt, in dem ein Anbieter eines Dienstes der Informationsgesellschaft niedergelassen ist. Dieser Mitgliedstaat hat die Einhaltung des Rechts im koordinierten Bereich (vgl. Art. 2 lit. h) ECRL) zu gewährleisten. Komplementär hierzu schließt Art. 3 Abs. 2 ECRL im Grundsatz aus, dass andere Mitgliedstaaten die Tätigkeit des Diensteanbieters in diesem Bereich einschränken.

Es existieren aber Ausnahmen vom Herkunftslandprinzip. In einigen Rechtsgebieten, etwa im Urheberrecht, findet es schon de lege lata keine Anwendung (Art. 3 Abs. 3 ECRL i.V.m. Anhang zur ECRL) und auch in anderen Bereichen kann die Tätigkeit bestimmter Diensteanbieter, die in einem anderen Mitgliedstaat niedergelassen sind, durchaus eingeschränkt werden. Einerseits sind in Art. 3 Abs. 4 lit. a) ECRL dafür materielle Vorgaben enthalten: Die einschränkende Maßnahme muss zum Schutz der öffentlichen Ordnung, Gesundheit, Sicherheit oder der Verbraucher erforderlich sein, weil der Diensteanbieter diese Schutzziele beeinträchtigt bzw. ernsthaft und schwerwiegend zu beeinträchtigen droht. Zudem muss sie in einem angemessenen Verhältnis zu den Schutzzielen stehen. Andererseits muss der jeweilige Mitgliedstaat prozedurale Vorgaben einhalten. Insb. muss er bereits vor Ergreifen der Maßnahme gewisse koordinative Handlungen vornehmen (Art. 3 Abs. 4 lit. b) ECRL), wenn nicht ein dringlicher Fall vorliegt (Art. 3 Abs. 5 ECRL).

Diskutiert wird ein Verstoß gegen das Herkunftslandprinzip immer wieder im Rahmen des NetzDG, da sein Anwendungsbereich in § 1 Abs. 1 auf eine Weise definiert wird, die einzig an die Tätigkeit der Diensteanbieter anknüpft. Aus dem persönlichen Anwendungsbereich ausgenommen sind nach § 1

[53] Zum Ganzen vgl. äußerst lesenswert: *von Kielmannsegg*, von Kielmannsegg, Gesetzgebung im Windschatten der Pandemie: § 287a SGB V und der Datenschutz in der Gesundheitsforschung, VerwArch 2021, 133, 141 ff. mwN.

Abs. 2 nur Anbieter, die weniger als zwei Millionen registrierte Nutzer in Deutschland haben. Der Ort ihrer Niederlassung findet also grundsätzlich keine Berücksichtigung.[54] Es fallen daher auch solche Diensteanbieter in den Kreis der Verpflichteten, die in einem anderen EU-Mitgliedstaat niedergelassen sind.[55] Die Anforderungen des NetzDG an diese Diensteanbieter unterfallen jedoch dem koordinierten Bereich i.S.d. Art. 2 lit. h) Ziff. i ECRL,[56] sodass im Grundsatz der Mitgliedstaat ihrer Niederlassung hierfür zuständig wäre, der für viele der relevanten Anbieter sozialer Medien, z.B. Facebook, nicht Deutschland ist.[57]

Der Gesetzgeber sieht für den Fall des NetzDG allerdings die Ausnahmeregelung des Art. 3 Abs. 4 lit. a) Ziff. i) ECRL als erfüllt an:[58] Das NetzDG wirke auf eine bessere Durchsetzung bestimmter Straftatbestände in sozialen Netzwerken hin, die dazu diene, das friedliche Zusammenleben der freien, offenen und demokratischen Gesellschaft zu schützen. Auch beziehe es sich auf einen bestimmten Dienst, nämlich speziell auf soziale Netzwerke. Es stehe zuletzt in einem angemessenen Verhältnis zum Schutzziel, da es der Verhinderung objektiv strafbaren Verhaltens diene.

Über die Vereinbarkeit des NetzDG mit dem Herkunftslandprinzip wird das VG Köln auf Klage von Google und Facebook entscheiden.[59] Eine Vorlage an den EuGH wäre zwecks Herstellung von Rechtssicherheit wünschenswert.

Für die zukünftig in § 5a NetzDG geregelten Auskunftspflichten der Anbieter sozialer Netzwerke gegenüber Forschern ergeben sich in dieser Hinsicht keine Besonderheiten.[60] Auch diese Pflichten fallen in den koordinierten Bereich nach Art. 2 lit. h) Ziff. i) ECRL, da sie neue Verhaltensanforderungen

---

[54] Anders nunmehr jedoch für Video-Sharing-Diensteanbieter, vgl. § 3e NetzDG.

[55] *Grünwald/Nüßing*, Vom NetzDG zum DSA: Wachablösung beim Kampf gegen Hate Speech?, MMR 2021, 283, 284; *Härting/Tekin*, Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG-E), IPRB 2020, 69, 71; *Hain/Ferreau/Brings-Wiesen*, Regulierung sozialer Netzwerke revisited, K&R 2017, 433, 434; *Peifer*, Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Zivilrechtliche Aspekte, AfP 2018, 14, 22; *Spindler*, Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz – europarechtswidrig?, ZUM 2017, 473, 474 f.; *ders.*, Das Netzwerkdurchsetzungsgesetz, K&R 2017, 533, 535; *ders.*, Rechtsdurchsetzung von Persönlichkeitsrechten, GRUR 2018, 365, 367.

[56] BR-Drs. 315/17, S. 9 f.; BT-Drs. 19/18792, S. 21; *Grünwald/Nüßing*, Vom NetzDG zum DSA: Wachablösung beim Kampf gegen Hate Speech?, MMR 2021, 283, 284; *Liesching*, Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG, MMR 2018, 26, 29.

[57] *Feldmann*, Zum Referentenentwurf eines NetzDG: Eine kritische Betrachtung, K&R 2017, 292, 296; *Härting/Tekin*, Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG-E), IPRB 2020, 69, 71; *Hain/Ferreau/Brings-Wiesen*, Regulierung sozialer Netzwerke revisited, K&R 2017, 433, 434; *Nölscher*, Das Netzwerkdurchsetzungsgesetz und seine Vereinbarkeit mit dem Unionsrecht, ZUM 2020, 301, 306 f.; *Peifer*, Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Zivilrechtliche Aspekte, AfP 2018, 14, 22.

[58] BR-Drs. 315/17, S. 9 f.; BT-Drs. 19/18792, S. 20 f.

[59] https://background.tagesspiegel.de/digitalisierung/google-koennte-das-netzdg-kippen, zuletzt abgerufen am 28.07.2021.

[60] So im Hinblick auf das Herkunftslandprinzip und die Reform des NetzDG, die keine Verschärfung der Pflichten der Diensteanbieter darstelle, sondern diese nur weiter fortentwickele, allgemein BT-Drs. 19/18297, S. 21; *Schwartmann*, Gesetzesrecht vor Hausrecht - Die geplanten Änderungen des NetzDG, MMR 2020, 501, 502; weiterhin kritisch jedoch *Liesching*, Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG, MMR 2020, 721, 721 f.; *ders.*, Das Herkunftslandprinzip der E-Commerce-Richtlinie und seine Auswirkung auf die aktuelle Mediengesetzgebung in Deutschland, 2020, S. 67 ff.

für Diensteanbieter enthalten.[61] Auch hierfür greift aber aus Sicht des Gesetzgebers die Ausnahme des Art. 3 Abs. 4 lit. a) ECRL, da die Forschung, die mithilfe der Auskünfte ermöglicht werde, der Verhütung von Straftaten sowie dem Verbraucherschutz diene.[62] Des Weiteren liege ein dringlicher Fall i.S.d. Art. 3 Abs. 5 ECRL vor, weil derzeit ein erhebliches Informationsdefizit über soziale Netzwerke bestehe, die einen zunehmend bedeutsamen öffentlichen Raum darstellten.[63] Diese Bedeutung sozialer Netzwerke hat jüngst auch der Generalanwalt am EuGH in seiner Stellungnahme zur Nichtigkeitsklage Polens gegen Art. 17 DSM-RL betont.[64]

[61] Dies aber offenlassend BT-Drs. 19/29392, S. 19.
[62] BT-Drs. 19/29392, S. 19.
[63] BT-Drs. 19/29392, S. 19.
[64] Schlussanträge des Generalanwalts v. 15.07.2021, C-401/19, Rn. 103.

VI. Datenschutzrechtlicher Rahmen

Werden personenbezogene Daten für Wissenschaft und Forschung zugänglich gemacht, sind neben den Vorgaben des Geschäftsgeheimnisschutzes und des Datenbankschutzes v.a. die Vorgaben des Datenschutzrechts zu achten. Bereits de lege lata kann ein Forschungsdatenzugang aber durchaus erfolgen, und dies selbst mit Blick auf sensible personenbezogene Daten i.S.d. Art. 9 DSGVO. Im Wesentlichen lässt sich ein Forschungsdatenzugang auf die folgenden Rechtsgrundlagen stützen:

1. Einwilligung

Die Weitergabe nicht-sensibler personenbezogener Daten kann auf Grundlage einer Einwilligung erfolgen, Art. 6 Abs. 1 S. 1 lit. a. Dabei gelten zunächst die allgemeinen Voraussetzungen, sodass die Einwilligung u.a. freiwillig, informiert und unmissverständlich erfolgen muss, Art. 4 Nr. 11, Art. 7 DSGVO. Soweit sensible Daten betroffen sind, ist eine ausdrückliche Einwilligung erforderlich, Art. 9 Abs. 1 DSGVO. Die betroffene Person muss bereits vor Erhebung der Daten über die beabsichtigte Datenverarbeitung und damit auch über die Weitergabe der Daten hinreichend informiert werden. Eine Einwilligung muss grundsätzlich für die konkrete Datenverarbeitung erteilt werden.[65] Häufig kann bei der Erhebung von Daten aber das spätere Forschungsvorhaben noch nicht konkret abgesehen werden.[66] Daher sollen im Rahmen wissenschaftlicher Forschung mit Blick auf ErwGr 33 weniger strenge Anforderungen an die Bestimmtheit der Einwilligung gelten.[67] Wie eine solche weniger bestimmte Einwilligungserklärung aber konkret auszugestalten ist, ist noch nicht umfassend ausdifferenziert. Die Medizininformatikinitiative hat für die medizinische Forschung einen Mustertext für die breite Einwilligung in die Sekundärnutzung pseudonymisierter Daten entwickelt, zu dem die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder am 15. April 2020 ihr Einverständnis erklärt hat.[68] Auf europäischer Ebene sieht der Entwurf des Data Governance Acts vor, dass die Anwendbarkeit derart standardisierter Einwilligungsformulare zur Erklärung eines „broad

[65] *Stemmer,* in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, DS-GVO Art. 7 Rn. 74 ff.
[66] So auch im Hinblick auf den Gesundheitssektor und epidemiologische Forschung *Pigeot*/*Buchner*, Epidemiologie und Datenschutz, DuD 2014, 816, 818.
[67] *Lauber-Rönsberg*, Rechtliche Aspekte des Forschungsdatenmanagements, in: Putnings/Neuroth/Neumann, Praxishandbuch Forschungsdatenmanagement, 2021, S. 104; *Stemmer,* in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, DS-GVO Art. 7 Rn. 78.
[68] Der Mustertext ist abrufbar unter: https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung, zuletzt abgerufen am 16.07.2021.

consents“ durch delegierten Rechtsakt für zulässig erklärt werden kann.[69] Denkbar sind auch Konzepte mehrstufiger oder dynamischer Einwilligung.[70] Diese Konzepte werden aber auch kritisch gesehen.[71]

2. Sekundärnutzung ohne Einwilligung

Eine Sekundärnutzung von Daten muss nicht zwingend auf eine Einwilligung gestützt werden. Auch weitere Erlaubnistatbestände kommen in Betracht.

a) Datenverarbeitung zur Aufgabenwahrnehmung im öffentlichen Interesse

Die Verarbeitung nicht-sensibler Daten lässt sich insb. auf Art. 6 Abs. 1 S. 1 lit. e und lit. f DSGVO stützen. Im Hinblick auf die Sekundärnutzung sensibler Daten sind zwingend die Vorgaben von Art. 9 DSGVO zu berücksichtigen. Art. 6 Abs. 1 S. 1 lit. e DSGVO kann dabei ausschließlich zur Rechtfertigung von Datenverarbeitungen durch öffentliche Stellen herangezogen werden. Dies können öffentliche Stellen des Bundes und der Länder, die sowohl öffentlich-rechtlich als auch privatrechtlich organisiert sein dürfen, sowie Beliehene sein, sofern eine Datenverarbeitung für eine der Stelle zugewiesenen öffentliche Aufgabe erforderlich ist. Eine solche Aufgabenzuweisung erfolgt durch rechtliche Vorgaben der Union oder der Mitgliedsstaaten, sodass Art. 6 Abs. 1 lit. e nicht als für sich alleinstehender Erlaubnistatbestand zu verstehen ist.[72] Die Norm verfolgt einen streng funktionalen Ansatz.[73] Sie rechtfertigt insb. Datenverarbeitungen zu Forschungszwecken durch Universitäten als öffentlich-rechtliche Forschungseinrichtungen, da diesen durch die Hochschulgesetze der Länder ausdrücklich Forschungsaufgaben zugewiesen werden.[74] Im Falle der Verarbeitung von sensiblen Daten sind die Vorgaben des Art. 9 Abs. 2 lit. g und lit. i DSGVO zu beachten, wonach für die Datenverarbeitung kein einfaches öffentliches Interesse mehr genügt, sondern ein erhebliches öffentliches Interesse vorausgesetzt wird.[75]

b) Datenverarbeitung auf Grundlage einer Interessenabwägung

Schließlich kann eine Datenverarbeitung zu wissenschaftlichen Zwecken auf Art. 6 Abs. 1 S. 1 lit. f DSGVO gestützt werden sowie für sensible Daten auf Art. 9 Abs. 2 lit. j DSGVO i.V.m. § 27 Abs. 1 S. 2

---

[69] Vorschlag der EU-Kommission v. 25.11.2020 für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Data Governance Act), abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767, zuletzt abgerufen am 16.07.2021.

[70] *Hummel/Braun/Augsberg/von Ulmenstein/Dabrock*, Datensouveränität - Governance-Ansätze für den Gesundheitsbereich, 2021, S. 10 u. 15, abrufbar unter: https://link.springer.com/content/pdf/10.1007%2F978-3-658-33755-1.pdf, zuletzt abgerufen am 16.07.2021.

[71] *Stemmer,* in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, DS-GVO Art. 7 Rn. 78.

[72] *Taeger,* in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, DSGVO Art. 6 Rn. 79 f.

[73] *Albers/Veit,* in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, DS-GVO Art. 6 Rn. 41; *Taeger,* in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, DSGVO Art. 6 Rn. 87.

[74] *Golla,* in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage, 2019, § 23 Rn. 43.

[75] *Taeger,* in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, DSGVO Art. 6 Rn. 87.

BDSG.[76] Art. 6 Abs. 1 lit. f DSGVO verlangt eine sorgfältige Abwägung zwischen den berechtigten Interessen des Verantwortlichen oder eines Dritten und den Interessen bzw. Grundrechten und Grundfreiheiten der betroffenen Person, bei der alle Umstände des Einzelfalls zu berücksichtigen sind.[77] Erforderlich ist i.R.v. Art. 6 Abs. 1 lit. f DSGVO zumindest eine Gleichrangigkeit der Interessen.[78] Zu diesen berechtigten Interessen können auch Forschungsinteressen des Verantwortlichen zählen. Öffentliche Stellen dürfen sich nur insoweit auf diesen Erlaubnistatbestand stützen, wie sie sich mit dem Betroffenen in keinem spezifisch staatlichen Verhältnis befinden, sondern als Teilnehmer im Privatrechtsverkehr gegenüberstehen (z.B. im Rahmen fiskalischer Hilfsgeschäfte).[79] Für privatrechtlich organisierte Forschungseinrichtungen gilt Art. 6 Abs. 1 lit. f DSGVO aber uneingeschränkt. Hingegen ist unklar, ob sich auch öffentliche Hochschulen auf diesen Erlaubnistatbestand stützen können.[80] Dies hängt von der Auslegung des Behördenbegriffs ab. Eine enge Auslegung stellt darauf ab, dass öffentliche Stellen, in denen nicht unmittelbar Hoheitsgewalt ausgeübt wird, nicht als Behörden i.S.d DSGVO angesehen werden sollten.[81] Dies beträfe insb. öffentlich-rechtliche Rundfunkanstalten, Religionsgemeinschaften oder eben öffentliche Universitäten. Eine weite Auslegung des Behördenbegriffes führte hingegen dazu, dass auch öffentliche Hochschulen als Behörden angesehen würden und sich insofern grds. nicht auf Art. 6 Abs. 1 lit. f DSGVO berufen könnten.[82]

Art. 9 Abs. 2 lit. j DSGVO i.V.m. § 27 BDSG differenziert nicht zwischen öffentlichen und nicht-öffentlichen Stellen. Vorausgesetzt wird, dass die Sekundärnutzung sensibler, personenbezogener Daten zu wissenschaftlichen Forschungszwecken erforderlich ist und dass die Forschungsinteressen die Interessen der Betroffenen erheblich überwiegen. Eine Verarbeitung nicht-anonymisierter Daten kann dann nicht mehr auf § 27 Abs. 1 BDSG gestützt werden, wenn die Zwecke auch durch die Arbeit mit anonymisierten Daten erreicht werden könnten.[83] Dies steht im Einklang mit der Anonymisierungspflicht in § 27 Abs. 3 BDSG, demgemäß die Daten zu anonymisieren sind, sobald dies mit dem verfolgten Zweck möglich bzw. zu vereinbaren ist. Jedenfalls hat eine gesonderte Speicherung der Zuordnungsmerkmale gem. § 27 Abs. 3 S. 2, 3 BDSG zu erfolgen. Für die Sekundärnutzung sensibler

[76] Vgl. auch: *Schlösser-Rost*/*Koch*, in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, BDSG § 27 Rn. 35 ff.
[77] *Taeger,* in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, DSGVO Art. 6 Rn. 98.
[78] *Schulz*, in: Gola, Datenschutz-Grundverordnung, 2. Auflage, 2018, Art. 6 Rn. 58; *Specht*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage, 2019, § 9 Rn. 50.
[79] *Albers/Veit,* in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, DS-GVO Art. 6 Rn. 46; vgl. dazu das Urteil des BVerwG v. 27.09.2018 - 7 C 5/17.
[80] *Lauber-Rönsberg*, Rechtliche Aspekte des Forschungsdatenmanagements, in: Putnings/ Neuroth/Neumann, Praxishandbuch Forschungsdatenmanagement, 2021, S. 107.
[81] So *Assion/Nolte/Veil*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar DSGVO, 2017, Art. 6 Rn. 124 ff.
[82] Dafür mit Blick auf Art. 6 Abs. 1 lit. e DSGVO und andere Sprachfassungen *Golla,* in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage, 2019, § 23 Rn. 45.
[83] *Taeger,* in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, BDSG § 27 Rn. 7.

Gesundheitsdaten sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person i.S.d. § 22 Abs. 2 BDSG zu treffen.[84]

Weiterhin setzt § 27 Abs. 1 BDSG voraus, dass die Forschungsinteressen die Interessen der Betroffenen erheblich überwiegen. Wann dies der Fall ist, ist noch nicht abschließend geklärt. Jedenfalls wird die allgemeine Abwägung aus Art. 6 Abs. 1 lit. f DSGVO dahingehend verschärft, dass die Darlegungslast dem Verantwortlichen obliegt und aufgrund des Zusatzes „erheblich" im Zweifel von einem Überwiegen der Interessen des Betroffenen auszugehen ist.[85] Jedenfalls ist eine Abwägung der widerstreitenden grundrechtlichen Positionen erforderlich.[86] Die Veröffentlichung sensibler, personenbezogener Daten ist nur unter zusätzlichen Voraussetzungen möglich, vgl. z.B. § 27 Abs. 4 BDSG. Soweit aber eine Weitergabe von Forschungsdaten nur gegenüber einem begrenzten Empfängerkreis erfolgt und die Weitergabe durch geeignete Maßnahmen wie z.B. Geheimhaltungsvereinbarungen o.ä. abgesichert ist, stellt dies keine Veröffentlichung dar und richtet sich nach § 27 Abs. 1 BDSG.[87]

c) Landesrechtliche Erlaubnistatbestände

Als weitere Erlaubnistatbestände kommen auf Landesebene § 11 Abs. 1 HmbDSG, § 17 Abs. 1 BlnDSG, § 13 Abs. 1 LDSG-BW (sowohl für die Verarbeitung sensibler Daten als auch nicht sensibler Daten) sowie Art. 8 BayDSG, § 13 Abs. 1 BremDSGVOAG, § 24 Abs. 1 HDSIG in Betracht (ausschließlich für die Verarbeitung sensibler Daten) in Betracht.[88] Gemäß § 11 I HmbDSG dürfen öffentliche Stellen für bestimmte Vorhaben der wissenschaftlichen und historischen Forschung sowie der Statistik personenbezogene Daten ohne Einwilligung verarbeiten, sofern schutzwürdige Interessen der betroffenen Personen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt sind. § 17 I BlnDSG erlässt der wissenschaftlichen und historischen Forschung und der Statistik ebenfalls das Erfordernis der Einwilligung in die Verarbeitung personenbezogener Daten. Voraussetzung dafür ist jedoch, dass das öffentliche Interesse an der Durchführung des Vorhabens die schutzwürdigen Belange der betroffenen Person erheblich überwiegt und der Zweck nicht auf eine andere Art und Weise erreicht werden kann. Nach § 13 Abs. 1 LDSG-BW

[84] Vgl. auch: *Schlösser-Rost/Koch,* in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, BDSG § 27 Rn. 35 ff.
[85] *Taeger,* in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, BDSG § 27 Rn. 8.
[86] *Taeger,* in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, BDSG § 27 Rn. 9; vgl. auch: *Schlösser-Rost/Koch,* in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, BDSG § 27 Rn. 31 ff.
[87] So *Lauber-Rönsberg*, Rechtliche Aspekte des Forschungsdatenmanagements, in: Putnings/ Neuroth/Neumann, Praxishandbuch Forschungsdatenmanagement, 2021, S. 106
[88] Ergänzend kann beispielsweise auch auf § 303e Abs. 1 Nr. 8 SGB V hingewiesen werden, der als Spezialvorschrift ebenfalls zur Grundlage einer Datenverarbeitung, nämlich der Weitergabe von Daten durch das Forschungsdatenzentrum, gemacht werden kann.

dürfen öffentliche Stellen personenbezogene Daten für wissenschaftliche oder historische Forschungszwecke verarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können und die Forschungsinteressen die Interessen des Betroffenen überwiegen. Die Regelung in Art. 8 BayDSG sieht im Wortlaut keine explizite Sonderregelung für die Forschung beim Umgang mit personenbezogenen Daten vor. Zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin können jedoch personenbezogene Daten verarbeitet werden, sofern dies erforderlich ist (Art. 8 Abs. 1 S. 1 Nr. 3). § 13 I BremDSGVOAG ermöglicht die Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Zwecken, soweit die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person am Unterbleiben der Verarbeitung erheblich überwiegen. Gleiches gilt für die Regelung des § 24 Abs. 1 HDSIG.

d) Zweckänderung, Art. 6 Abs. 4 DSGVO

Eine zweckändernde Verarbeitung für im öffentlichen Interesse liegende Archivzwecke für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke ist ebenfalls nach Art. 6 Abs. 4 DSGVO möglich. Es wird von der Vereinbarkeit der Sekundärnutzung mit dem Ursprungszweck der Verarbeitung der personenbezogenen Daten ausgegangen. Dabei sind aber die in Art. 89 Abs. 1 DSGVO aufgeführten Voraussetzungen zu berücksichtigen,[89] insb. technische und organisatorische Maßnahmen müssen bestehen, mit denen u.a. die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.

VII. Regulierungsstruktur und gesetzliche Grundlagen des nationalen Forschungsdatenzugangsregimes de lege lata

1. Regulierungsstruktur

Ein Datenzugang für die Wissenschaft unabhängig von bereits bestehenden vertraglichen Beziehungen und ebenfalls unabhängig von datenschutzrechtlichen Betroffenenrechten des einzelnen Forschers[90] kann über fünf strukturell verschiedene Regulierungsinstrumente erreicht werden, nämlich durch

1. Einen grundrechtsunmittelbaren Datenzugangsanspruch zugunsten der Forschung

2. Echte Forschungsklauseln

[89] *Taeger*, in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, DSGVO Art. 6 Rn. 154.

[90] Ausschließlich zum Zweck der besseren Lesbarkeit wird im vorliegenden Gutachten auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen.

3. Open-Data-Gesetzgebung

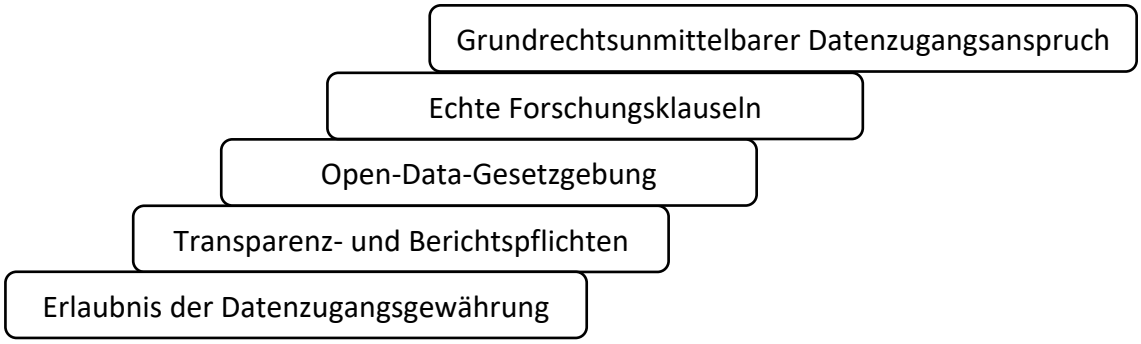
4. Transparenzregelungen und Berichtspflichten

5. Erlaubnisse der Datenzugangsgewährung

Diese fünf Wege zu einem Datenzugang wirken unterschiedlich intensiv zugunsten von Forschung und Wissenschaft. Transparenzvorgaben und Berichtspflichten finden sich über viele Gesetze verteilt v.a. gegenüber privaten Institutionen, beispielsweise in § 2 NetzDG gegenüber Anbietern Sozialer Netzwerke und Videosharingplattform-Diensten. Sie stellen recht allgemein gehaltene Informationen zur Verfügung, die in der Wissenschaft zwar verwertet werden können, aber mangels Spezifität der Daten nicht von erheblichem Interesse sein dürften. Transparenzregelungen und Berichtspflichten dienen vielmehr der breiten Öffentlichkeit zur eher allgemeinen Information.[91] Für die Zwecke von Wissenschaft und Forschung sind aber detailliertere Angaben und Rohdaten erforderlich (z.B. die in § 5a Abs. 6 NetzDG ausdrücklich genannten Daten, ihr jeweiliger Kontext und die Trainingsdaten der automatisierten Verfahren[92], um eigenständig wissenschaftlich fundierte Erkenntnisse zu den fraglichen Verfahren zur automatisierten Erkennung von Inhalten zu gewinnen). Open-Data Gesetzgebung adressiert v.a. die öffentliche Verwaltung, so etwa durch das E-Government-Gesetz (EGovG) und verpflichtet hier zur Offenlegung von Daten gegenüber einem nicht auf Wissenschaft und Forschung beschränkten Personenkreis. Eine Datenzugangsgewährung fordert zumindest dann, wenn sie personenbezogene Daten betrifft, eine datenschutzrechtliche Verarbeitungsgrundlage. Diese Erlaubnis einer Datenzugangsgewährung begründet keinen materiell-rechtlichen Anspruch auf Datenzugang und wirkt daher ebenfalls nur begrenzt zugunsten von Wissenschaft und Forschung. Materiell-rechtliche Ansprüche auf Datenzugang werden allein durch sog. echte Forschungsklauseln begründet. Weitreichender könnte nur ein grundrechtsunmittelbarer Datenzugangsanspruch sein, dessen Existenz auf Grundlage von Informations- und Forschungsfreiheit entsprechend dem vom Bundesverwaltungsgericht anerkannten presserechtlichen Informationsanspruch diskutiert werden soll. Entsprechend ihrer Wirkintensität ergibt sich eine Stufenleiter des Datenzugangs:[93]

[91] Vgl. BT-Drs. 19/29392, S. 18.
[92] BT-Drs. 19/29392, S. 18.
[93] Begrifflichkeit angelehnt an die Stufenleiter der Gestattungen bei *Ohly*, Volenti non fit iniuria - Die Einwilligung im Privatrecht, 2002, S. 141 ff.

Abb. 2: Stufenleiter des Datenzugangs



2. Gesetzliche Grundlagen eines Forschungsdatenzugangs

Den nachfolgenden Ausführungen vorangestellt ist die Diskussion um einen grundrechtsunmittelbaren Datenzugangsanspruch für Wissenschaft und Forschung auf Grundlage von Informations- und Forschungsfreiheit (nachfolgend Unterpunkt a). Das Instrument der Open-Data Gesetzgebung soll im Rahmen dieser Untersuchung jedenfalls überblicksartig dargestellt werden (nachfolgend Unterpunkt b), ohne dass der Schwerpunkt der Untersuchung auf diesem Themenkomplex liegt. Auch die Ansprüche aus den Informationsfreiheitsgesetzen des Bundes und der Länder werden in diesem Zusammenhang zusammenfassend dargestellt. Es handelt sich jedoch bei ihnen um allgemeine Informationszugangsansprüche, die nicht wissenschaftsspezifisch wirken und daher ebenso wie kartell- und datenschutzrechtliche Regelungen vernachlässigt werden. Dies gilt auch für Transparenz- und Berichtspflichten als lediglich unspezifisches und den Interessen von Wissenschaft und Forschung nicht in ausreichendem Maße dienendes Instrument der Gesetzgebung.

Im Mittelpunkt der hier vorgenommenen Untersuchung stehen aufgrund ihrer Wirkintensität zugunsten von Wissenschaft und Forschung die echten Forschungsklauseln. Sie sollen im Folgenden exemplifiziert und ausdifferenziert werden, um die existenten Datenzugangsansprüche auf ihre Voraussetzungen zu untersuchen und so letztlich Best-Practice-Regelungen für ein Forschungsdatenzugangsgesetz identifizieren zu können (nachfolgend Unterpunkt c.). Eine solche echte Forschungsklausel i.S.e. subjektiven Datenzugangsrechts beinhaltet nicht per se eine datenschutzrechtliche Verarbeitungserlaubnis, die aber für den Fall, dass personenbezogene Daten vom Zugangsrecht betroffen sind, explizit in das subjektive Zugangsrecht aufgenommen werden könnte. Häufig ist ein Datenzugang zugunsten von Wissenschaft und Forschung datenschutzrechtlich bereits de lege lata gestattet und in der Regel sollte die Normierung eines subjektiven Datenzugangsrechtes so ausgelegt werden können, dass der Gesetzgeber ein generelles Überwiegen der Interessen des Zugangsberechtigten i.S.d. Art. 6 Abs. 1 lit. f DSGVO bzw. Art. 9 Abs. 2 lit. h DSGVO i.V.m. § 27 BDSG anerkennt und eine Verarbeitung daher basierend auf diesen Rechtsgrundlagen für

zulässig hält. Die Aufnahme einer Klausel zur Erlaubnis der Datenzugangsgewährung in die Forschungsklausel wäre aus Gründen der Rechtssicherheit aber sinnvoll.

Z.T. kann aber durchaus auch eine explizite datenschutzrechtliche Rechtsgrundlage für den Datenzugang erforderlich sein, wie der BGH dies für eine Datenübermittlung im Rahmen eines Auskunftsanspruches in seinem Urteil Ärztebewertung I aufgrund von § 12 Abs. 2 TMG entschieden hat.[94] § 12 TMG bleibt auch nach Inkrafttreten des TTDSG bestehen und gibt vor, dass der Diensteanbieter für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke (also auch für die Datenzugangsgewährung zum Zwecke von Forschung und Wissenschaft) nur verwenden darf, soweit das TMG oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

Um einen entsprechenden Regelungsgehalt in künftige Datenzugangsansprüche integrieren zu können, sind die Erlaubnisse der Datenzugangsgewährung ebenfalls im Rahmen dieser Studie zu analysieren. Es kann aber, sofern eine Norm wie § 12 Abs. 2 TMG, der eine Verankerung im Gesetz fordert, nicht vorliegt, auch in der Gesetzesbegründung klargestellt werden, dass das subjektive Zugangsrecht zugleich die datenschutzrechtliche Befugnis zur Gewährung des Datenzugangs beinhalten soll, was z.B. die Gesetzesbegründung zu § 8 Krebsregistergesetz-E[95] oder auch zu § 303e SGB V[96] zeigt.

a) Grundrechtsunmittelbarer Datenzugangsanspruch

aa) Grundrechtsunmittelbarer Anspruch aus Art. 5 Abs. 1 GG

Ein grundrechtsunmittelbarer Anspruch auf Datenzugang auf Grundlage der Informationsfreiheit, Art. 5 Abs. 1 Alt. 2 GG wird de lege lata überwiegend abgelehnt.[97] Gegebenenfalls kann sich ein gegen den Staat gerichteter Anspruch auf eine Eröffnung von Informationsquellen aber aus anderen Grundrechten ergeben. Ein solcher grundrechtsunmittelbarer Anspruch steht der Presse nach ständiger Rechtsprechung des BVerwG gegen *Bundes*behörden[98] zu.[99] Er soll im Folgenden näher erläutert werden, um anschließend seine Übertragbarkeit auf die Forschungsfreiheit zu prüfen.

---

[94] BGH, Urteil v. 1.7.2014 – VI ZR 345/13 – Ärztebewertung I.

[95] https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/K/Krebsregisterdaten-GE_Kabinett.pdf, S. 48, zuletzt abgerufen am 16.07.2021.

[96] BT-Drs. 19/13438 zu Art. 1 Nr. 39 (§303e).

[97] BVerwG CR 1986, 835; BayVGH NJW 19851663, 1664; OVG RP, NJW 1984, 1135, 1136; OVG NRW CR 1986, 834; *Havel*, Informationszugangsansprüche des forschenden Wissenschaftlers, S. 93 f.; *Kempen*, in: Epping/Hillgruber, BeckOK Grundgesetz, 41. Edition, 2019, Art. 5 Rn. 32.

[98] Zum Behördenbegriff *Burkhardt*, in: Löffler, PresseR, 6. Auflage, 2015, § 4 LPG Rn. 55 ff.

[99] BVerwG, NVwZ 2013, 1006, 1007 Rn. 17; NJW 2014, 1126, 1128 Rn. 23; NVwZ 2015, 1383 Rn. 6; NVwZ 2015, 1388, 1390 Rn. 24; NVwZ 2016, 945 Rn. 10 f.; NVwZ 2016, 1020, 1021 Rn. 16; NVwZ 2016, 1023, 1024 Rn. 12; Beschl. v. 17.11.2016 – Az. 6 A 3.15, BeckRS 2016, 113717 Rn. 12; Beschl. v. 21.09.2016 – Az. 6 A 10.14, BeckRS 2016, 54085 Rn. 8; ZD 2017, 483,

Die Pressefreiheit gemäß Art. 5 Abs. 1 S. 2 Var. 1 GG verpflichtet die Legislative, die Rechtsordnung so auszugestalten, dass der Presse ihre funktionsgemäße Betätigung ermöglicht wird.[100] Dies erfordert es, dass die Pressevertreter einen Auskunftsanspruch gegenüber sämtlichen Behörden erhalten, damit sie entsprechend der den Medien von der Verfassung zugewiesenen Aufgabe die Arbeit staatlicher Stellen kontrollieren und der Allgemeinheit hierüber Bericht erstatten können.[101]

Gegenüber den *Landes*behörden ist der (Landes-)Gesetzgeber seiner Verpflichtung zur Gewährleistung von Auskunftsansprüchen dadurch nachgekommen, dass er einen Auskunftsanspruch einfachgesetzlich kodifiziert hat: Für die Pressevertreter wird dieser in den LPresseG (i.d.R. in § 4 Abs. 1 LPresseG[102]) gewährt, für die Rundfunkvertreter ist er in § 5 Abs. 1 S. 1 MStV normiert und für die Anbieter von Telemedien in § 18 Abs. 4 i.V.m. § 5 Abs. 1 S. 1 MStV. Ein vergleichbarer Auskunftsanspruch gegenüber Bundesbehörden existiert im einfachen Recht dagegen nicht. Aus dem Grund folgt der Anspruch der Pressevertreter auf Auskunft gegenüber diesen Behörden unmittelbar aus der Pressefreiheit.[103]

Zu berücksichtigen ist jedoch, dass dem Gesetzgeber bei der Kodifikation von Auskunftsansprüchen eine Ausgestaltungsprärogative zukommt. Um dieses Vorrecht nicht zu unterlaufen, kann auf der Grundlage von Art. 5 Abs. 1 S. 2 Var. 1 GG nur ein Minimalstandard an Auskünften gewährt werden. Dies ist jener Standard, den auch der Gesetzgeber, der den Auskunftsanspruch einfachgesetzlich normieren würde, mindestens gewähren müsste.[104] Der verfassungsunmittelbare Anspruch kann demnach nur so weit gehen, wie der Auskunft keine berechtigten schutzwürdigen Interessen Privater oder öffentlicher Stellen an der Vertraulichkeit der begehrten Informationen entgegenstehen.[105] Solche Interessen lassen sich beispielhaft den Ausschlussgründen für die einfachgesetzlichen Auskunftsansprüche der Medien entnehmen.[106] Danach kann die Auskunftserteilung z.B. verweigert werden, wo sie die sachgemäße Durchführung eines schwebenden Verfahrens beeinträchtigen oder vereiteln würde (siehe etwa § 4 Abs. 2 Nr. 1 LPresseG B-W, § 18 Abs. 1 S. 2 Nr. 1 MStV).

484 Rn. 9; NVwZ 2018, 414, 415 f. Rn. 17; NVwZ 2018, 902, 903 Rn. 14; NVwZ 2018, 907, 908 Rn. 15; NVwZ 2019, 479, 480 Rn. 11; NVwZ 2020, 1368, 1370 Rn. 28; offengelassen allerdings in BVerfG, NJW 2014, 3711, 3712 Rn. 26; NVwZ 2016, 50, 51 Rn. 12.

[100] BVerwG, NVwZ 2013, 1006, 1008 Rn. 27; NJW 2014, 1126, 1127 Rn. 22.

[101] BVerwG, NVwZ 2013, 1006, 1008 f. Rn. 27; NJW 2014, 1126, 1127 f. Rn. 22; NVwZ 2016, 1020, 1021 Rn. 17; NVwZ 2019, 479, 480 Rn. 13.

[102] Siehe aber § 5 Abs. 1 BbgPresseG, § 3 Abs. 1 S. 1 HessPresseG, § 12a Abs. 1 LMG RhPf, § 5 Abs. 1 SMG.

[103] BVerwG, NVwZ 2013, 1006, 1009 Rn. 29; NVwZ 2015, 1388, 1390 Rn. 24.

[104] BVerwG, NVwZ 2013, 1006, 1009 Rn. 29; NJW 2014, 1126, 1128 Rn. 23; NVwZ 2015, 1388, 1390 Rn. 26.

[105] BVerwG, NVwZ 2013, 1006, 1009 Rn. 29; NJW 2014, 1126, 1128 Rn. 23; NVwZ 2015, 1383 Rn. 6; NVwZ 2015, 1388, 1390 Rn. 24; NVwZ 2016, 945 Rn. 12; NVwZ 2016, 1020, 1021 Rn. 16; NVwZ 2016, 1023, 1024 Rn. 23; Beschl. v. 21.09.2016 – Az. 6 A 10.14, BeckRS 2016, 54085 Rn. 10; ZD 2017, 483, 484 Rn. 11; NVwZ 2018, 414, 416 Rn. 18; NVwZ 2018, 902, 904 Rn. 16; NVwZ 2018, 907, 908 Rn. 16; NVwZ 2019, 479, 480 Rn. 13; NVwZ 2020, 1368, 1370 Rn. 28.

[106] BVerwG, NVwZ 2013, 1006, 1009 Rn. 29.

Der Katalog der kodifizierten Ausschlussgründe ist im Hinblick auf den verfassungsunmittelbaren Auskunftsanspruch aber einerseits nicht abschließend.[107] Andererseits folgt daraus, dass der Gesetzgeber einen Ausschlussgrund im einfachen Recht vorgesehen hat, nicht per se, dass bei Vorliegen dieses Grundes auch der verfassungsunmittelbare Auskunftsanspruch ausgeschlossen ist.[108] Vielmehr bedarf es einer Prüfung im Einzelfall, ob die Sicherung der funktionsgemäßen Betätigung der Presse es gebietet, deren Informationsinteresse höher zu gewichten als die entgegenstehenden Vertraulichkeitsinteressen.[109] Dabei verlangt die Pressefreiheit prinzipiell, das für eine Auskunft streitende Informationsinteresse staatlicherseits nicht inhaltlich zu gewichten und zu bewerten. Es obliegt vielmehr der Presse, nach publizistischen Kriterien zu entscheiden, ob eine Information von öffentlichem Interesse ist.[110]

Auf Rechtsfolgenseite ist der Auskunftsanspruch im Grundsatz auf die mündliche oder schriftliche Beantwortung konkreter Fragen gerichtet.[111] Seine Erfüllung kann im Einzelfall aber auch die Gewährung von Akteneinsicht voraussetzen, wenn andere Formen des Informationszugangs hinsichtlich der begehrten Information unsachgemäß wären und – etwa bei besonders komplexen Zusammenhängen – nur durch eine Akteneinsicht eine vollständige und wahrheitsgemäße Sachverhaltskenntnis vermittelt werden kann.[112]

Dabei ist der Auskunftsanspruch stets dahingehend beschränkt, dass die Auskunftsverpflichteten nur tatsächlich bei ihnen vorhandene Daten und Informationen herausgeben müssen. Damit sind solche Informationen gemeint, die zum Zeitpunkt des Auskunftsbegehrens tatsächlich vorliegen. Es obliegt ihnen dagegen nicht, die begehrten Daten und Informationen erst durch eine Sachverhaltserforschung bzw. weitere Untersuchungen zu generieren.[113]

bb) Grundrechtsunmittelbarer Datenzugangsanspruch aus Art. 5 Abs. 3 GG

Um der Forschung einen entsprechenden Anspruch zuzusprechen, müsste entsprechend den Vorgaben des BVerwG die Tätigkeit der Forschung einen Datenzugang erfordern und die Forschungsfreiheit gemäß Art. 5 Abs. 1 S. 2 Var. 1 GG die Legislative in ihrer objektiv-rechtlichen Dimension dazu verpflichten, die Rechtsordnung so auszugestalten, dass der Forschung diese funktionsgemäße Betätigung ermöglicht wird.[114] Anders als die Presse ist der Forschung aber gerade

[107] BVerwG, NVwZ 2013, 1006, 1009 Rn. 29.
[108] BVerwG, NVwZ 2015, 1388, 1390 f. Rn. 27, Rn. 29; NVwZ 2016, 945 f. Rn. 15.
[109] BVerwG, NVwZ 2015, 1388, 1390 f. Rn. 27, Rn. 29; NVwZ 2016, 945 f. Rn. 15; NVwZ 2016, 1020, 1021 ff. Rn. 16, Rn. 20 ff.
[110] BVerwG, NVwZ 2016, 1020, 1022 Rn. 18 f. S. auch BVerwG, NVwZ 2018, 414, 416 Rn. 18; NVwZ 2018, 902, 904 Rn. 16; NVwZ 2018, 907, 908 Rn. 16.
[111] BVerwG, NVwZ 2020, 1368, 1370 Rn. 31. Vgl. auch schon BVerwG, NJW 2015, 1126, 1128 Rn. 24.
[112] BVerwG, NVwZ 2020, 1368, 1370 Rn. 31.
[113] BVerwG, NVwZ 2013, 1006, 1009 Rn. 30, Rn. 32; Beschl. v. 17.11.2016 – Az. 6 A 3.15, BeckRS 2016, 113717 Rn. 12; Vgl. auch BVerfG, NVwZ 2016, 50, 51 Rn. 15 f.
[114] BVerwG, NVwZ 2013, 1006, 1008 Rn. 27; NJW 2014, 1126, 1127 Rn. 22.

nicht die Aufgabe des „Public Watchdog“ zugewiesen. Es handelt sich vielmehr um eine Tätigkeit mit dem Ziel der Gewinnung neuer Erkenntnisse, die jedenfalls in vielerlei Hinsicht auch stattfinden kann, ohne dass ein Datenzugangsanspruch gegenüber Behörden existiert. Zwar ließe sich möglicherweise jedenfalls für bestimmte Forschungsgegenstände ein solcher funktionsspezifischer verfassungsunmittelbarer Datenzugangsanspruch herleiten,[115] er steht jedoch auf äußerst unsicherer Grundlage und wäre in seinem Anwendungsbereich entsprechend dem verfassungsunmittelbaren presserechtlichen Auskunftsanspruch äußerst begrenzt. Ausreichend für einen privilegierten Forschungsdatenzugang der Wissenschaft wäre er nicht.

b) Open-Data-Gesetzgebung und Informationsfreiheitsgesetze

aa) PSI-Richtlinie und EGovG

Die Open-Data Gesetzgebung, die auf nationaler Ebene von einer „Open-Data Strategie“ geleitet wird, soll die Nutzungspotentiale von Verwaltungs- und Forschungsdaten heben.[116] Um dieses Ziel zu realisieren, existieren sowohl auf nationaler als auch auf Unionsebene gesetzgeberische Entwicklungen, die Grundlage und Rechtsrahmen für Open-Data bilden. Hierzu gehören v.a. die PSI-Richtlinie und das EGovernment-Gesetz (EGovG).

Bereits die PSI-Richtlinie aus dem Jahr 2003 intendierte die bessere (Wieder)Nutzung von Daten. Sie wurde durch die RL 2013/37/EU grundlegend überarbeitet und in den Folgejahren auf Grundlage einer öffentlichen Anhörung[117] und einem Impact Assessment[118] reflektiert. 2019 wurde die PSI-Richtlinie ein weiteres Mal angepasst (RL (EU) 2019/1024). Die Umsetzung der aktuellen Fassung der PSI-Richtlinie zum 16.07.2021 erfolgt durch das Datennutzungsgesetz (DNG), welches das Informationsweiterverwendungsgesetz (IWG) ablöst. Während mit dem DNG die Weiterverwendung von Daten geregelt wird, normiert § 12a EGovG eine Datenbereitstellungspflicht durch die Verwaltung. Mit dem EGovG wurden ursprünglich Forderungen aus dem G8-Aktionsplan umgesetzt und eine Open-Data-Regelung auf Bundesebene geschaffen, die initial die Behörden der unmittelbaren Bundesverwaltung dazu verpflichtete, die von ihnen erhobenen „Rohdaten“, also unbearbeitete Daten, grundsätzlich zu veröffentlichen, sodass diese Daten von jeder Person und auch von anderen

[115] Einen grundrechtsunmittelbaren Anspruch auf Datenzugang entsprechend dem presserechtlichen Informationsanspruch fordert etwa: *Havel*, Informationszugangsansprüche des forschenden Wissenschaftlers, S. 98 ff.
[116] *Bundesregierung*, Open-Data-Strategie der Bundesregierung v. 12.07.2021, S. 6, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/open-data-strategie-der-bundesregierung.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 16.07.2021.
[117] https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-revision-directive-reuse-public-sector-information, zuletzt abgerufen am 16.07.2021.
[118] Impact Assessment on the review of the Directive 2003/98/EC on the reuse of public sector information, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-review-directive-200398ec-reuse-public-sector-information, zuletzt abgerufen am 16.07.2021.

Verwaltungsorganen unentgeltlich genutzt werden können.[119] Mit dem 1. Open-Data-Fortschrittsbericht der Bundesregierung wurde am 02.10.2019 erstmalig die Regelung des § 12a EGovG reflektiert und Fortschritte sowie zukünftige Herausforderungen bei der Umsetzung zusammengefasst.[120] Eine weitere Weichenstellung wurde im gleichen Zeitraum mit dem 2. Nationalen Aktionsplan am 04.09.2019 beschlossen[121], der aufgrund der Mitgliedschaft Deutschlands im Open Government Partnership (OGP) erstellt wurde. Das OGP ist eine internationale Initiative von 78 Mitgliedsstaaten, die sich für die Förderung von offenem Regierungs- und Verwaltungshandeln einsetzt. Die Erkenntnisse aus dem 1. Open-Data-Fortschrittsbericht sowie dem 2. Nationalen Aktionsplan bilden die Grundlage für die Weiterentwicklung von Open-Data im Verlauf der aktuellen 19. Legislaturperiode und fanden auch Eingang in die Open-Data Strategie der Bundesregierung.[122]

Zur Verbesserung der Datennutzbarkeit sieht das 2. Open Data Gesetz, das das DNG beinhaltet, [123] die Verwendung maschinenlesbarer Formate von Daten verpflichtend vor. Zentral ist auch, dass durch die Neufassung des § 12a EGovG erstmals auch die mittelbare Bundesverwaltung sowie Forschungsdaten der Bereitstellungspflicht unterliegen.[124] So werden bestimmte Bereiche der Daseinsvorsorge[125] in den Anwendungsbereich integriert und zur Bereitstellung dynamischer Daten[126] sowie hochwertiger Datensätze verpflichtet.[127] Außerdem sollen in allen Bundesbehörden (mit mehr als 50 Beschäftigten) Open-Data-Koordinatoren eingesetzt und die Bereitstellungsprozesse und Datenformate durch eine Verordnung verbessert und standardisiert werden.

Gleichzeitig steht seit dem 01.09.2018 das Kompetenzzentrum für Open Data (CCOD) , das dem Bundesverwaltungsamt unterstellt ist, als Ansprechpartner für alle Fragen im Hinblick auf die

[119] Eingehend zur Regelung in § 12a EGovG: *Richter,* „Open Government Data" für Daten des Bundes, NVwZ 2017, 1408-1413.
[120] Siehe BT-Drs. 19/14140.
[121] Zweiter Nationaler Aktionsplan zur Teilnahme an der OGP, abrufbar unter: https://www.open-government-deutschland.de/opengov-de/open-government-partnership/aktionsplaene-und-berichte/zweiter-nationaler-aktionsplan-1591034, zuletzt abgerufen am 16.07.2021.
[122] *Bundesregierung*, Die Open-Data Strategie der Bundesregierung, S. 1-32, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/open-data-strategie-der-bundesregierung.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 16.07.2021.
[123] Für einen Überblick über das Gesetzgebungsverfahren siehe https://dip.bundestag.de/vorgang/gesetz-zur-änderung-des-e-government-gesetzes-und-zur-einführung-des-gesetzes/273941, zuletzt abgerufen am 16.07.2021.
[124] Zur Einbeziehung öffentlich finanzierter Forschungsdaten siehe *Zimmermann,* Zum Potenzial des europäischen Weiterverwendungsrechts für die Erforschung der Biodiversität, ZUR 2021, 84, 87 ff.
[125] Welche Bereiche damit im Einzelnen gemeint sind, geht aus der Gesetzesbegründung nicht hervor. Jedenfalls erweitert das DNG den Anwendungsbereich auf öffentliche Unternehmen der Daseinsvorsorge aus den Bereichen Wasser, Energie und Verkehr, siehe hierzu BT-Drs. 141/21, S. 13.
[126] Dynamische Daten sind Aufzeichnungen in digitaler Form, die häufig oder in Echtzeit aktualisiert werden (meistens aufgrund ihrer Volatilität oder ihres raschen Verhaltens).
[127] Ausführlich zu den Auswirkungen der PSI-Richtlinie auf öffentliche Unternehmen *Buchholz,* Die neue PSI-Richtlinie – Wieviel Datenhoheit verbleibt den öffentlichen Unternehmen?, IR 2019, 197-206.

Aufbereitung und Veröffentlichung von Daten und die Anbindung an das nationale Metadatenportal GovData zur Verfügung.[128] Außerdem ist es Kontaktstelle für die Open-Data Stellen der Länder.

In bestimmten Bereichen gab es darüber hinaus auch auf Unionsebene bereits in der Vergangenheit Rechtsakte und Initiativen zur öffentlichen Bereitstellung von Datensätzen. Dies gilt beispielsweise für die IVS-Richtlinie 2010/40/EU[129], die der Einrichtung intelligenter Verkehrssysteme im Straßenverkehr dienen soll, die INSPIRE-Richtlinie2007/2/EG[130], die den Aufbau einer Geodateninfrastruktur bezweckt, und das Gemeinsame Umweltinformationssystem (SEIS)[131], das Umweltdaten für eine Überwachungsinfrastruktur „gebrauchstauglich" erfassen und archivieren soll. Außerdem existiert auf europäischer Ebene ein Datenportal, das die Metadaten innerhalb der EU veröffentlichter Datensätze sammelt. So wird der Zugang zu öffentlichen Daten der Datenportale verschiedener Mitgliedsstaaten erleichtert, indem diese anhand der Metadaten, also bspw. bestimmter Schlagworte und Sachgebiete, miteinander verknüpft werden.

Anders als auf europäischer Ebene, auf der schon nach Art. 42 GRCh ein einklagbarer Anspruch der EU-Bürger auf Zugang zu Verwaltungsdaten der Union und ihrer Organe, Einrichtungen und Stellen besteht,[132] fehlt ein solcher Anspruch im EGovG, vgl. § 12a Abs. 1 S. 2 EGovG. Ansprüche auf bestimmte Daten staatlicher Stellen bestehen aber nach dem Informationsfreiheitsgesetz (IFG), dem Umweltinformationsgesetz (UIG) und dem Verbraucherinformationsgesetz (VIG) sowie entsprechender landesrechtlicher Regelungen. Sie sollen im Folgenden kursorisch erläutert werden:

bb) Zugang zu amtlichen Informationen nach dem Informationsfreiheitsgesetz (IFG)

Ein Anspruch auf Zugang zu amtlichen Informationen ergibt sich aus § 1 Abs. 1 IFG sowie aus den Informationsfreiheitsgesetzen der Bundesländer.[133]

[128] https://www.govdata.de, zuletzt abgerufen am 16.07.2021.
[129] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:DE:PDF, zuletzt abgerufen am 16.07.2021.
[130] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32007L0002&from=de, zuletzt abgerufen am 16.07.2021.
[131] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008SC0112:DE:HTML, zuletzt abgerufen am 16.07.2021.
[132] Dazu *Jarass*, in: Jarass, EU-Grundrechte-Charta, 4. Auflage, 2021, Art. 42 Rn. 2.
[133] Baden-Württemberg: Landesinformationsfreiheitsgesetz (LIFG); Berlin: Berliner Informationsfreiheitsgesetz (IFG Berlin); Brandenburg: Akteneinsichts- und Informationszugangsgesetz (AIG); Bremen: Bremer Informationsfreiheitsgesetz (BremIFG); Hamburg: Hamburgisches Transparenzgesetz (HmbTG); Hessen: Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG); Mecklenburg-Vorpommern: Informationsfreiheitsgesetz (IFG M-V); Nordrhein-Westfalen: Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW); Rheinland-Pfalz: Landestransparenzgesetz (LTranspG); Saarland: Saarländisches Informationsfreiheitsgesetz (SIFG); Sachsen-Anhalt: Informationszugangsgesetz Sachsen-Anhalt (IZG LSA); Schleswig-Holstein: Informationszugangsgesetz für das Land Schleswig-Holstein (IZG-SH); Thüringen: Thüringer Transparenzgesetz (ThürTG).

Der Kreis der Anspruchsinhaber ist nach allen IFG weit gefasst. Nach dem IFG des Bundes und einigen Landes-IFG ist „jeder" anspruchsberechtigt[134] Teilweise wird dies in den Landes-IFG noch konkretisiert, indem als mögliche Anspruchsinhaber natürliche Personen und juristische Personen des Privatrechts (§ 1 S. 1 IZG-SH) bzw. jeder Mensch und jede juristische Person (§ 3 Abs. 1 IFG Berlin) sowie Personenvereinigungen (§ 1 Abs. 2 S. 2 IFG M-V), nicht rechtsfähige Vereinigungen von Bürgerinnen und Bürgern (§ 2 Abs. 1 S. 2 LTranspG, § 4 Abs. 1 ThürTG), Bürgerinitiativen sowie Verbände zur Beeinflussung öffentlicher Angelegenheiten (§ 9 Abs. 1 AIG), Zusammenschlüsse, soweit diese organisatorisch hinreichend verfestigt sind (§ 3 Nr. 1 LIFG), bzw. juristische Personen des öffentlichen Rechts, soweit diese Grundrechtsträger sind (§ 2 Abs. 1 S. 3 LTranspG), festgelegt werden. Das IFG NRW wiederum ist enger gefasst und gewährt den Anspruch lediglich jeder natürlichen Person (§ 4 Abs. 1 IFG NRW).

In den Kreis der Anspruchsverpflichteten fallen gemäß dem IFG des Bundes alle Behörden (§ 1 Abs. 1 S. 1 IFG), wobei nicht der Behördenbegriff des § 1 Abs. 4 VwVfG entscheidend ist, sondern ein funktionales Begriffsverständnis zugrunde zu legen ist.[135] Dies wird im IFG des Bundes noch auf sonstige Bundesorgane und -einrichtungen ausgeweitet, soweit diese öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen (§ 1 Abs. 1 S. 2 IFG), und auf natürliche oder juristische Personen des Privatrechts erstreckt, soweit eine Behörde sich ihrer zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient (§ 1 Abs. 1 S. 3 IFG). Die Landes-IFG enthalten vergleichbare, teils aber deutlich ausdifferenziertere Regelungen. Zusammengefasst werden darin sowohl die unmittelbare als auch die mittelbare Landesverwaltung sowie die Kommunen verpflichtet und der Kreis der Anspruchsgegner teilweise ausdrücklich noch auf bestimmte private Stellen ausgeweitet, die öffentliche Aufgaben wahrnehmen.

Anspruchsgegenstand sind gemäß dem IFG des Bundes amtliche Informationen (§ 1 Abs. 1 S. 1 IFG). Diese sind in § 2 Nr. 1 IFG definiert als jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung. Ausgenommen sind Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen. Diese oder eine ähnliche Definition verwenden auch die meisten Landes-IFG. Etwas elaborierter ist bspw. die schleswig-holsteinische Regelung, nach der Informationen alle auf Informationsträgern bei informationspflichtigen Stellen vorhandenen Zahlen, Daten, Fakten, Erkenntnisse oder sonstige Auskünfte sind (§ 2 Abs. 1 Nr. 1 IZG S-H). Enger wiederum ist in sachlicher Hinsicht das Akteneinsichts- und Informationszugangsgesetz (AIG), nach dem nur ein Akteneinsichtsrecht besteht. Akten sind gemäß § 3 AIG alle schriftlich, elektronisch, optisch, akustisch oder auf andere Weise aufgezeichneten Unterlagen, soweit sie ausschließlich amtlichen oder dienstlichen Zwecken dienen. Ausgenommen erneut Entwürfe und Notizen, die nicht Bestandteil des

[134] Ähnlich gemäß § 1 Abs. 2 HmbTG, wonach der Anspruch jeder Person zusteht.
[135] BVerwG, ZD 2012, 84, 85 Rn. 11; ZD 2012, 346, 347 Rn. 11.

Vorgangs sind und spätestens nach dessen Abschluss vernichtet werden. Vergleichbar eng gefasst ist der Auskunftsanspruch nach dem IFG Berlin, der auf Einsicht in oder Auskunft über den Inhalt von Akten gerichtet ist. Dies sind gemäß § 3 Abs. 2 IFG Berlin alle schriftlich, elektronisch, optisch, akustisch oder auf andere Weise festgehaltenen Gedankenverkörperungen und sonstigen Aufzeichnungen, soweit sie amtlichen Zwecken dienen. Die möglichen Themen, auf die sich die beanspruchten Aufzeichnungen oder Akten beziehen können, werden in den verschiedenen IFG nicht weiter eingeschränkt.

cc) Zugang zu Umweltinformationen nach dem Umweltinformationsgesetz (UIG)

In persönlicher sowie sachlicher Hinsicht enger ausgestaltet ist der Zugangsanspruch zu Umweltinformationen. Es existieren sowohl ein UIG des Bundes als auch entsprechende Gesetze aller Bundesländer.[136] Zwischen diesen bestehen jedoch deutlich weniger Unterschiede als zwischen Bund- und Landes-IFG: Einige Landesvorschriften erklären das UIG des Bundes mit wenigen Modifikationen für anwendbar,[137] andere sind dem UIG des Bundes jedenfalls nachempfunden.[138]

Anspruchsberechtigt ist nach dem UIG des Bundes sowie den meisten Landesgesetzen jede Person, was natürliche Personen ebenso einschließt wie juristische Personen des Privatrechts.[139] Dem stehen nicht rechtsfähige Personenvereinigungen gleich, die organisatorisch hinreichend verfestigt sind.[140] Auch für bestimmte juristische Personen des öffentlichen Rechts ist die Anspruchsberechtigung nach der Rechtsprechung anerkannt: Anspruchsberechtigt ist danach eine Gemeinde, die sich bei der Antragstellung in einer mit „Jedermann" vergleichbaren Informationslage gegenüber den informationspflichtigen Stellen befindet und örtliche Aufgaben wahrnimmt.[141] Auch für eine Religionsgemeinschaft wurde dies bejaht.[142] In Übertragung der in diesen Fällen entwickelten Leitlinien wird in der Literatur vertreten, dass auch andere verselbstständigte grundrechtsberechtigte Verwaltungsträger, etwa die Universitäten, in den Kreis der Anspruchsberechtigten fallen sollen.[143]

---

[136] Baden-Württemberg: Umweltverwaltungsgesetz (UVwG); Bayern: Bayerisches Umweltinformationsgesetz (BayUIG); Brandenburg: Umweltinformationsgesetz des Landes Brandenburg (BbgUIG); Bremen: Umweltinformationsgesetz für das Land Bremen (BremUIG); Hamburg: Hamburgisches Umweltinformationsgesetz (HmbUIG); Hessen: Hessisches Umweltinformationsgesetz (HUIG); Mecklenburg-Vorpommern: Landes-Umweltinformationsgesetz (LUIG M-V); Niedersachen: Niedersächsisches Umweltinformationsgesetz (NUIG); Nordrhein-Westfalen: Umweltinformationsgesetz Nordrhein-Westfalen (UIG NRW); Saarland: Saarländisches Umweltinformationsgesetz (SUIG); Sachsen: Sächsisches Umweltinformationsgesetz (SächsUIG); Sachsen-Anhalt: Umweltinformationsgesetz des Landes Sachsen-Anhalt (UIG LSA); Thüringen: Thüringer Umweltinformationsgesetz (ThürUIG). In Berlin wurde mit § 18a IFG Berlin eine spezielle Vorschrift ins allgemeine IFG eingeführt. In Rheinland-Pfalz wurde der Auskunftsanspruch nach dem LTranspG in dessen § 1 Abs. 1 explizit auf Umweltinformationen ausgedehnt. Auch das allgemeine IZG S-H regelt sowohl den Zugang zu amtlichen Informationen generell als auch speziell zu Umweltinformationen.

[137] Siehe etwa § 18a IFG Berlin.

[138] Siehe etwa das HUIG.

[139] So die Gesetzesbegründung zum UIG des Bundes, BT-Drs. 15/3406, S. 15.

[140] BVerwG, NVwZ 1999, 1220; NVwZ 2008, 791, 793 Rn. 22.

[141] BVerwG, NVwZ 2008, 791, 794 Rn. 28 ff.; NVwZ 2017, 1775, 1777 Rn. 34 ff.

[142] BVerwG, NVwZ 2008, 791, 794 Rn. 26 f.

[143] Siehe dafür nur *Reidt/Schiller*, in: Landmann/Rohmer, UmweltR, 94. Ergänzungslieferung, 2020, § 3 UIG Rn. 7 mwN.

Darauf deuten auch die wenigen vom UIG des Bundes abweichenden Landesgesetze hin: Nach § 2 Abs. 1 S. 2, S. 3 LTranspG sind anspruchsberechtigt natürliche und juristische Personen des Privatrechts, nicht rechtsfähige Vereinigungen von Bürgerinnen und Bürgern und juristische Personen des öffentlichen Rechts, soweit sie Grundrechtsträger sind. Gemäß § 3 S. 1 IZG S-H fällt darunter jede natürliche oder juristische Person, was prima facie auch solche des öffentlichen Rechts erfassen kann.

Informationspflichtig und damit nach § 3 Abs. 1 S. 1 UIG bzw. den korrespondierenden landesrechtlichen Vorschriften anspruchsverpflichtet sind, erstens, die Regierung sowie andere Stellen der öffentlichen Verwaltung. Explizit in den Kreis der Anspruchsverpflichteten aufgenommen werden hiernach auch Gremien, die beratend für diese Stellen tätig sind; sie gelten als Teil der Stelle, die ihre Mitglieder beruft. Ausdrücklich ausgenommen sind dagegen Legislativ- und Judikativtätigkeiten der grundsätzlich verpflichteten Stellen. Zweitens sind auch natürliche und juristische Personen des Privatrechts anspruchsverpflichtet, soweit sie öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen, die im Zusammenhang mit der Umwelt stehen und dabei staatlicher Kontrolle unterliegen (s. exemplarisch zu alledem nur § 2 Abs. 1 UIG).

Anspruchsgegenstand sind Umweltinformationen, wobei diese im exemplarisch heranzuziehenden § 2 Abs. 3 UIG des Bundes als Daten über bestimmte Kategorien definiert werden. Erfasst sind Daten über den Zustand von Umweltbestandteilen und die Wechselwirkungen zwischen diesen, über Faktoren, die sich auf jene Umweltbestandteile (wahrscheinlich) auswirken, über Maßnahmen oder Tätigkeiten, die sich auf jene Umweltbestandteile oder Faktoren (wahrscheinlich) auswirken bzw. den Schutz der Umweltbestandteile bezwecken, über Berichte über die Umsetzung des Umweltrechts, über Kosten-Nutzen-Analysen oder sonstige wirtschaftliche Analysen und Annahmen, die zur Vorbereitung oder Durchführung der genannten Maßnahmen oder Tätigkeiten verwendet werden, und über den Zustand der menschlichen Gesundheit und Sicherheit, die Lebensbedingungen des Menschen, Kulturstätten und Bauwerke, soweit sie vom Zustand der Umweltbestandteile oder den Faktoren, Maßnahmen oder Tätigkeiten betroffen sind bzw. sein können.

dd) Zugang zu Daten nach dem Verbraucherinformationsgesetz (VIG)

Ebenfalls sachlich wie persönlich gegenüber dem allgemeinen Auskunftsanspruch eingeschränkt ist der Informationsanspruch nach § 2 Abs. 1 S. 1 VIG.

Anspruchsberechtigt ist nach dem Wortlaut dieser Norm „jeder“. Insbesondere ist der Kreis der Anspruchsberechtigten nicht auf Verbraucher beschränkt. Er umfasst jedenfalls alle natürlichen Personen sowie juristischen Personen des Privatrechts.[144] Umstritten ist die Anspruchsberechtigung

[144] Weiter („jeder natürlichen oder juristischen Person“) aber noch die Gesetzesbegründung, BT-Drs. 16/5404, S. 10.

für nicht rechtlich verbundene Personenvereinigungen.[145] Für juristische Personen des öffentlichen Rechts wird sie in der Rechtsprechung im Grundsatz abgelehnt. Eine Ausnahme wird aber für grundrechtsberechtigte Personen des öffentlichen Rechts wie etwa Rundfunkanstalten gemacht.[146]

Der Kreis der Anspruchsverpflichteten wird durch § 2 Abs. 2 VIG legaldefiniert. Hierunter fallen einerseits alle Behörden i.S.d. § 1 Abs. 4 VwVfG, denen gesetzlich die Wahrnehmung öffentlich-rechtlicher Aufgaben oder Tätigkeiten zugewiesen ist, die entweder der Erfüllung der in § 1 LFGB genannten Zwecke oder, bei Verbraucherprodukten, in der Gewährleistung der Sicherheit und Gesundheit nach den produktsicherheitsrechtlichen Vorschriften dienen. Auf der anderen Seite sind hiervon alle natürlichen oder juristischen Personen des Privatrechts erfasst, für die dies gilt und die der Aufsicht einer Behörde unterstellt sind. Gewisse Behörden mit bestimmten Aufgaben, insbesondere legislativer oder judikativer Tätigkeit, werden durch § 2 Abs. 3 VIG explizit aus dem Kreis der Anspruchsverpflichteten ausgenommen.

Gegenstand des Anspruchs gemäß § 2 Abs. 1 S. 1 VIG sind bestimmte Kategorien von Daten. Dies sind z.B. Daten über festgestellte Abweichungen von lebensmittel-, futtermittel- oder produktsicherheitsrechtlichen Anforderungen und Maßnahmen bzw. Entscheidungen diesbezüglich, über gewisse zugelassene Abweichungen hiervon, über Gefahren bzw. Risiken für die Gesundheit und Sicherheit von Verbrauchern, die von Erzeugnissen und Verbraucherprodukten ausgehen, sowie über bestimmte Eigenschaften dieser Erzeugnisse und Verbraucherprodukte, über ausgewählte Verhaltensweisen diesbezüglich, z.B. ihre Kennzeichnung, über Ausgangsstoffe und die bei der Gewinnung angewendeten Verfahren, über Überwachungsmaßnahmen sowie andere behördliche Schritte zum Schutz von Verbrauchern und bestimmte Statistiken.

ee) Verhältnis der Ansprüche nach IFG, UIG und VIG zu § 12a EGovG

Nach § 12a Abs. 1 S. 1 EGovG stellen die Behörden der unmittelbaren Bundesverwaltung unbearbeitete Daten, die sie zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben erhoben haben oder durch Dritte in ihrem Auftrag haben erheben lassen, zum Datenabruf über öffentlich zugängliche Netze bereit. Nach § 12a Abs. 5 EGovG müssen diese Daten grundsätzlich maschinenlesbar bereitgestellt und mit Metadaten versehen werden, die im nationalen Metadatenportal GovData einzustellen sind. Die (technische) Form der Auskunftserteilung ist im IFG, UIG oder VIG dagegen nicht verbindlich geregelt. Nach § 1 Abs. 2 S. 1 IFG des Bundes kann der Auskunftsverpflichtete Akteneinsicht gewähren oder die Informationen in sonstiger Weise zur Verfügung stellen. Gemäß § 3 Abs. 2 S. 1 UIG des Bundes und § 6

[145] Siehe dazu nur *Heinicke*, in: Zipfel/Rathke, LebensmittelR, 178. Ergänzungslieferung, 2020, § 2 VIG Rn. 10 mwN.
[146] OVG Lüneburg, LMuR 2015, 211, 214 Rn. 12; vgl. auch BVerfG, NVwZ 2009, 1556, 1557.

Abs. 1 S. 1 VIG kann der Zugang zu der begehrten Information durch Auskunftserteilung, Gewährung von Akteneinsicht oder in sonstiger Weise eröffnet werden.

Ein Anspruch auf die Bereitstellung von Daten besteht nach § 12a Abs. 1 S. 2 EGovG nicht. Die Anspruchsberechtigten der erörterten Auskunftsansprüche haben allerdings auch im Anwendungsbereich des § 12a EGovG einen Anspruch auf Zugang zu den von IFG, UIG und VIG erfassten Daten an sich nach Maßgabe dieser Gesetze. Die Bereitstellung dieser Informationen im nach § 12a Abs. 5 EGovG vorgesehenen Format können sie gemäß § 12a Abs. 1 S. 2 EGovG allerdings nicht verlangen.

c) Echte Forschungsklauseln

Datenzugang für die Forschung ließe sich am effektivsten durch die Verankerung echter Forschungsklauseln gewährleisten. Hierbei ist zu unterscheiden zwischen privatrechtlichen und öffentlich-rechtlichen Forschungsklauseln, d.h. solchen Klauseln, die eine private Stelle als Zugangsadressaten definieren und solchen, die eine öffentlich-rechtliche Stelle adressieren.

aa) Privatrechtlicher Datenzugangsanspruch

(1) System originärer und abgeleiteter Forschungsklauseln

Wird Datenzugang gegenüber privaten Stellen durch ein subjektives Recht auf Datenzugang gewährt, lässt sich diese Forschungsklausel abgeleitet oder originär ausgestalten. Abgeleitet ist sie, wenn sie an bestehende Datenzugangsansprüche angelehnt wird, die Forschung also dem bereits gesetzlich privilegierten Zugangsadressaten gleichgestellt wird, so wie dies bei § 19 Abs. 3 UrhG der Fall ist. Originär ist die Forschungsklausel, wenn sie ohne Vorbild eines anderen Zugangsadressaten einen Datenzugangsanspruch zugunsten der Wissenschaft begründet, wie dies bei § 5a NetzDG der Fall ist. Auch Art. 31 DSA-E enthält eine originäre Forschungsklausel.

(2) Ausübung datenschutzrechtlicher Befugnisse in Vertretung des Betroffenen

Auch die Normen des Datenschutzrechts, die einen Auskunftsanspruch und einen Anspruch auf Datenübertragbarkeit gegen private und öffentliche Stellen normieren, können einen Forschungsdatenzugang gewährleisten, wenn die auf Grundlage dieser Normen erhaltenen Daten der Forschung zugeführt werden, z.B. über die „Datenspende“ oder aber, wenn die Ansprüche auf Auskunft und Datenübertragbarkeit übertragbar oder jedenfalls in Stellvertretung ausgeübt werden könnten. Eine „Datenspende“ ist nichts anderes als die Übermittlung von Daten auf Grundlage der Einwilligung des Betroffenen. Sie ist daher grundsätzlich möglich, als alleiniges Instrument eines Datenzugangs in ihrer Effektivität aber fraglich. Die Übertragbarkeit datenschutzrechtlicher Befugnisse im Wege der Abtretung ist abzulehnen. Eine translatorische Übertragung der Betroffenenrechte würde

dazu führen, dass diese vom Betroffenen selbst nicht mehr ausgeübt werden könnten, was mit dem informationellen Selbstbestimmungsrecht, das dem Datenschutzrecht als Schutzgut auch unter der Datenschutzgrundverordnung entgegen v.a. in jüngster Vergangenheit aufkommender Stimmen noch immer zugrunde liegt,[147] nicht gerecht würde. Anders zu beurteilen ist allerdings eine Stellvertretung mit Blick auf die datenschutzrechtlichen Betroffenenrechte. Der DSGVO ist die Geltendmachung der Betroffenenrechte durch Dritte grundsätzlich bekannt: So sieht Art. 80 Abs. 1 DSGVO vor, dass Betroffene eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht beauftragen können, in ihrem Namen eine Beschwerde einzureichen, oder die in den Art. 77, 78 und 79 DSGVO genannten Rechte und das Recht auf Schadensersatz gemäß Art. 82 DSGVO in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist. Art. 80 Abs. 1 DSGVO gewährleistet ausweislich seines Wortlauts zwar nicht die Geltendmachung der Art. 15 ff. DSGVO durch Dritte. Teleologische Argumente sprechen aber dennoch für die Möglichkeit einer Ausübung der Betroffenenrechte in Stellvertretung: Für Betroffene ist dies effektiver als die eigene Geltendmachung der Betroffenenrechte, weil sie sich der Drittexpertise bedienen können. Teleologisch wäre es daher nicht nachvollziehbar, wenn ein Rechtsakt, der primär dem Schutz des Betroffenen in Ansehung der ihn betreffenden personenbezogenen Daten dient, diesen Rückgriff auf Dritte nicht zuließe. Weshalb ein solcher Rechtsakt nach Sinn und Zweck zwar bei der gerichtlichen Durchsetzung von Sekundäransprüchen sowie bei der aufsichtsbehördlichen Rechtsdurchsetzung den Rückgriff auf Dritte Personen zulassen sollte, wie dies im Art. 80 DSGVO vorgesehen ist, nicht jedoch bei der außergerichtlichen Durchsetzung der Betroffenenrechte, die häufig erst die Kenntnis von einer rechtswidrigen Datenverarbeitung herbeiführen (Art. 15 DSGVO) und Sekundäransprüche damit erst ermöglichen, ist nur schwerlich begründbar. Richtigerweise wird daher vermehrt vertreten, dass auch Ansprüche auf Information, Auskunft und Unterlassung gegen Verantwortliche und Auftragsverarbeiter für die betroffene Person geltend gemacht werden können.[148] Mit diesen Rechten sollte es aber nicht sein Bewenden haben. Mit der dargelegten teleologischen Argumentation eines primär verfolgten Betroffenenschutzes[149] sollten vielmehr sämtliche Betroffenenrechte der Art. 15 ff. DSGVO sowie der Einwilligungswiderruf durch Dritte geltend gemacht werden können.[150]

---

[147] Eindrucksvoll *Trute*, in: Roßnagel, Handbuch Datenschutzrecht, 1. Auflage, 2003, Kap. 2 Rn. 6: *„mehrdimensionales Konzept, das sein Gravitationszentrum in der kommunikativen Selbstbestimmung der Persönlichkeit hat und deren Leitbild nicht das Datengeheimnis, sondern die Wahrung von Selbstbestimmung in einer Datenverkehrsordnung ist“*; zustimmend *Franzius*, Das Recht auf informationelle Selbstbestimmung, ZJS 2015, 259, 266; auch der EuGH hat seine Entscheidung „Google Spain“ im Wesentlichen auf Art. 7 GrCh und nicht auf Art. 8 GrCh gestützt, vgl. EuGH, Urteil v. 13.5.2014 - C-131/12 = ECLI:EU:C:2014:317 (Google Spain), Rn. 80 ff.

[148] *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, 3. Auflage, 2020, Art. 80 DSGVO Rn. 11; *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, 1, 11 f.

[149] *Pötters*, in: Gola, DS-GVO, 2. Auflage, 2018, Art. 1 DSGVO Rn. 8.

[150] *Specht-Riemenschneider*/*Blankertz* et al., Die Datentreuhand, MMR-Beilage 2021, 25, 42 mwN.

Wie auch die Datenspende erfordert die Beauftragung zur Wahrnehmung der Betroffenenrechte in Vertretung das Tätigwerden des Betroffenen. Die Zusammenführung großer Datenbestände wird auf dieser Grundlage kaum gelingen, dennoch sollte die Möglichkeit, Betroffenenrechte in Stellvertretung auszuüben, als unterstützendes Instrument eines umfassenderen Forschungsdatenzugangsregimes gesetzlich verankert werden.

bb) Öffentlich-rechtlicher Datenzugangsanspruch

Verpflichten echte Forschungsklauseln, ausschließlich Stellen des öffentlichen Rechts, handelt es sich um öffentlich-rechtliche Datenzugangsansprüche. Sie müssen unterschieden werden in gebundene Entscheidungen und Ansprüche auf ermessensfehlerfreie Entscheidung.

(1) Gebundene Entscheidungen

Im Falle einer gebundenen Entscheidung ist die zugangsverpflichtete Stelle des öffentlichen Rechts stets an die gesetzlich vorgesehene Rechtsfolge – hier die Datenzugangsgewährung – gebunden. Sie sind in der Regel formuliert als „Muss-Regelungen“ oder „Ist-Regelungen“. Ein entsprechender Anspruch findet sich in § 303e SGB V. Danach hat ein Forschungsdatenzentrum die ihm vom Spitzenverband Bund der Krankenkassen und von der Vertrauensstelle übermittelten Daten den Institutionen der Gesundheitsversorgungsforschung, den Hochschulen, den nach landesrechtlichen Vorschriften anerkannten Hochschulkliniken, öffentlich geförderten außeruniversitären Forschungseinrichtungen und sonstigen Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung unter bestimmten Voraussetzungen zugänglich zu machen.

Ein Anspruch auf die Nutzung öffentlichen Archivgutes findet sich in § 10 BArchG sowie in den entsprechenden landesrechtlichen Archivgesetzen, z.B. § 3 LArchG RLP.[151] Der Anspruch ist nicht spezifisch auf die Forschung beschränkt, sondern kann von jedermann geltend gemacht werden. Zugunsten der Forschung können aber z.B. Sperrfristen verkürzt werden, vgl. § 3 Abs. 4 Nr. 3 LArchG RLP.

Letztlich ergibt sich ein originärer Datenzugangsanspruch auch aus § 32 StUG, wonach für die Forschung zum Zwecke der politischen und historischen Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes oder der Herrschaftsmechanismen der ehemaligen Deutschen Demokratischen Republik oder der ehemaligen sowjetischen Besatzungszone der Bundesbeauftragte auf Antrag bestimmte Unterlagen zur Verfügung stellt.

[151] Nutzungsregelungen der weiteren Landesarchive: § 6 LArchG BW; § 6 LArchG NRW; § 9 LArchG SH; § 9 BbgArchivG; Art. 10 BayArchivG; § 9 SächsArchivG; § 10 ArchG LSA; § 5 NArchG; § 11 SArchG; § 5 HamArchG; § 7 BremArchivG; § 8 ArchGB; § 16 ThürArchivG; § 12 HArchivG; § 9 LArchivG MV.

(2) Anspruch auf ermessensfehlerfreie Entscheidung über den Datenzugang

Ansprüche auf ermessenfehlerfreie Entscheidung über den Datenzugang sind hingegen als „Soll-Regeln“ oder „Kann-Regeln“ ausgestaltet.

(a) Rechtsgrundlagen

Entsprechende Regelungen finden sich in

- Art. 3 der Verordnung 557/2013 über europäische Statistiken in Bezug auf den Zugang zu vertraulichen Daten für wissenschaftliche Zwecke, wonach die Kommission Zugang zu vertraulichen Daten für wissenschaftliche Zwecke gewähren kann, die sich zur Entwicklung, Erstellung und Verbreitung europäischer Statistiken in ihrem Besitz befinden.

- § 8 Abs. 1 Krebsregistergesetz-E, der als „Soll-Regelung“ (eingeschränkter Ermessensspielraum) ein Recht auf ermessensfehlerfreie Entscheidung über den Zugang zu Krebsregisterdaten zu wissenschaftlichen Forschungszwecken normiert. Auf landesrechtlicher Ebene existiert Art. 13 BayKRegG, wonach das Bayerische Landesamt für Gesundheit und Lebensmittelsicherheit (LGL) Dritten auf Antrag gestatten kann, anonymisierte Daten zu nutzen und in diesem Rahmen Daten übermittelt, soweit ein berechtigtes, insb. wissenschaftliches Interesse glaubhaft gemacht wird.

- § 363 Abs. 3 i.V.m. § 303e Abs. 2 Nr. 7, 8 SGB V, der einen Anspruch auf ermessensfehlerfreie Entscheidung über den Zugang zu Daten aus der elektronischen Patientenakte gewährt.

- § 150b GewO, wonach die Registerbehörde Hochschulen, anderen Einrichtungen, die wissenschaftliche Forschung betreiben, und öffentlichen Stellen Auskunft aus dem Register erteilen kann, soweit diese für die Durchführung bestimmter wissenschaftlicher Forschungsarbeiten erforderlich ist.

- § 88a AufenthaltsG-E, wonach das Bundesamt für Migration und Flüchtlinge bestimmte personenbezogene Daten staatlichen oder staatlich anerkannten Hochschulen und anderen Forschungseinrichtungen übermitteln darf, deren Tätigkeit überwiegend aus öffentlichen Mitteln finanziert wird, soweit dies für die Durchführung eines wissenschaftlichen Forschungsvorhabens über Integrationsfragen erforderlich ist und weitere Voraussetzungen erfüllt sind.

- § 66 PStG, wonach Hochschulen, anderen Einrichtungen, die wissenschaftliche Forschung betreiben, und öffentlichen Stellen Auskunft aus einem oder Einsicht in ein Personenstandsregister sowie Durchsicht von Personenstandsregistern gewährt werden kann, wenn dies für die Durchführung bestimmter wissenschaftlicher Forschungsvorhaben erforderlich ist.

- § 16 Abs. 6 BStatG, wonach das Statistische Bundesamt und die statistischen Ämter der Länder für die Durchführung wissenschaftlicher Vorhaben Hochschulen oder sonstigen Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung Einzelangaben übermitteln dürfen, wenn die Einzelangaben nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können (faktisch anonymisierte Einzelangaben) oder auch innerhalb speziell abgesicherter Bereiche des Statistischen Bundesamtes und der statistischen Ämter der Länder Zugang zu formal anonymisierten Einzelangaben gewähren dürfen, wenn wirksame Vorkehrungen zur Wahrung der Geheimhaltung getroffen werden. Berechtigte können allerdings nur Amtsträger oder Amtsträgerinnen, oder für den öffentlichen Dienst besonders Verpflichtete sein. Auch nach landesrechtlichen Vorschriften können Einzelangaben zu Forschungszwecken übermittelt werden, z.B. auf Grundlage von § 16 LStatG BW.

(b) Berücksichtigung der Forschungsfreiheit bei der Ermessensausübung

Auch wenn sich aus der Forschungsfreiheit selbst jedenfalls de lege lata kein Datenzugangsanspruch begründen lässt, so ist der objektive Grundrechtsgehalt doch jedenfalls bei der Ermessensausübung zu berücksichtigen. Die Forschungsfreiheit ist zumindest in die Ermessensentscheidung einzustellen, im Einzelfall kann sich auch eine Ermessensreduzierung auf null ergeben,

> *„wenn das wissenschaftliche Zugangsinteresse alle schutzwürdigen Gesichtspunkte so deutlich überwiegt, dass eine Zugangsverweigerung unter jedem Blickwinkel unverhältnismäßig wäre.“*[152]

3. Erlaubnis der Datenzugangsgewährung

Neben diesen echten Forschungsklauseln existieren im privatrechtlichen Bereich diverse Erlaubnisse der Datenzugangsgewährung, die kein subjektives Recht für den Zugangsberechtigten begründen, sondern lediglich als Rechtsgrundlage die Datenübermittlung an Forschung und Wissenschaft gestatten. Diese Rechtsgrundlage ist in der Regel datenschutzrechtlicher Natur.

Erlaubnisse der Datenzugangsgewährung finden sich in:

- § 27 BDSG, der gemeinsam mit Art. 9 Abs. 1 lit. h DSGVO die Verarbeitung sensibler Daten für wissenschaftliche Forschungszwecke für rechtmäßig erklärt

- § 476 StPO, der regelt, unter welchen Voraussetzungen in einem Strafverfahren rechtmäßig erhobene personenbezogene Daten (insb. in Form von Akten) für Zwecke wissenschaftlicher Forschung übermittelt und verwendet werden dürfen. I.V.m. § 186 SVollzG gelten diese Voraussetzungen und

[152] *Hevers*, Informationszugangsansprüche des forschenden Wissenschaftlers, S. 424.

Rechtsfolgen auch für Strafvollzugsakten. Es handelt sich nach wohl überwiegender Ansicht nicht um eine materiell-rechtliche Anspruchsgrundlage.[153]

- § 98 SGB XI, wonach die Pflegekassen mit Erlaubnis der Aufsichtsbehörde die Datenbestände leistungserbringer- und fallbeziehbar für bestimmte Forschungsvorhaben selbst auswerten und aufbewahren dürfen.

- § 119 SGB XII, wonach der Träger der Sozialhilfe einer wissenschaftlichen Einrichtung, die im Auftrag des Bundesministeriums für Arbeit und Soziales ein Forschungsvorhaben durchführt, das dem Zweck dient, die Erreichung der Ziele von Gesetzen über soziale Leistungen zu überprüfen oder zu verbessern, Sozialdaten übermitteln darf.

- § 42a BZRG, wonach eine Übermittlung personenbezogener Daten aus dem Register an Hochschulen und andere Einrichtungen, die wissenschaftliche Forschung betreiben, unter bestimmten Voraussetzungen zulässig ist.

- § 75 SGB X, wonach eine Übermittlung von Sozialdaten unter bestimmten Voraussetzungen zulässig ist, soweit sie erforderlich ist für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich oder der wissenschaftlichen Arbeitsmarkt- und Berufsforschung oder der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben.

- § 67c Abs. 5 SGB X, wonach erhobene Sozialdaten zur Durchführung eines bestimmten Vorhabens der wissenschaftlichen Forschung oder Planung im Sozialleistungsbereich verwendet werden dürfen.

- § 14 Abs. 2a, 15g TPG, wonach Ärzte und anderes wissenschaftliches Personal des Entnahmekrankenhauses, des Transplantationszentrums, der Koordinierungsstelle und der Vermittlungsstelle personenbezogene Daten, die von dem jeweiligen Entnahmekrankenhaus, dem jeweiligen Transplantationszentrum oder der jeweiligen Stelle nach § 11 oder § 12 TPG im Rahmen der Organ- und Spendercharakterisierung beim Organ- oder Gewebespender oder im Rahmen der Organ- oder Gewebeübertragung beim Organ- oder Gewebeempfänger erhoben oder an diese übermittelt worden sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten dürfen. § 15g erlaubt die Übermittlung von pseudonymisierten oder anonymisierten Daten zu Forschungszwecken.

- § 24a Abs. 1 AZRG, wonach das Bundesamt für Migration und Flüchtlinge bestimmte gespeicherte Daten zu Ausländern, die keine freizügigkeitsberechtigten Unionsbürger sind, verarbeiten darf, soweit dies für die Durchführung bestimmter wissenschaftlicher Forschungsvorhaben erforderlich ist.

[153] Str. vgl. insb. *Wittig*, in: Graf, BeckOK StPO, 39. Edition, 2021, § 476 Rn. 1; a.A. *Singelstein*, in: Knauer/Kudlich/Schneider, MüKo StPO, 1. Auflage, 2014, § 476 Rn. 1; *Puschke/Weßlau*, in: Wolter, SK-StPO, 5. Auflage, 2017, § 476 Rn. 2.

- § 34 SächsKHG, der beispielhaft auch für andere Landeskrankenhausgesetze benannt wird und wonach Ärzte Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer Klinik oder in sonstigen medizinischen Einrichtungen, in den Universitätsklinika oder in sonstigen medizinischen Einrichtungen gespeichert sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten und nach Abs. 2 und 3 unter gewissen Voraussetzungen auch übermitteln dürfen.[154]

- § 35 Abs. 7 HMG, wonach zum Zwecke unabhängiger wissenschaftlicher Forschung die Meldebehörden personenbezogene Daten ohne Einwilligung der Betroffenen für bestimmte Forschungsvorhaben übermitteln dürfen, soweit die schutzwürdigen Belange der Betroffenen wegen der Art der Verwendung nicht beeinträchtigt werden.

- § 88a Abs. 4 AufenthaltsG, der es dem Bundesamt für Migration und Flüchtlinge erlaubt teilnehmerbezogene Daten über die Anmeldung, die Dauer der Teilnahme und die Art des Abschlusses von berufsbezogenen Deutschsprachförderungsprogrammen mit staatlichen oder staatlich anerkannten Hochschulen und anderen Forschungseinrichtungen, die überwiegend aus öffentlichen Mitteln finanziert werden, zu teilen.

4. Normen mit unklarem Anspruchs-/Erlaubnischarakter

Der Charakter der folgenden Normen ist unklar. Sie normieren in ihrem Wortlaut eher eine Erlaubnis der Datenzugangsgewährung. Aus der Gesetzesbegründung oder aber aus der Rechtsnatur ergibt sich aber, dass auch auf einen Datenzugangsanspruch geschlossen werden könnte

- § 63a Abs. 5 StVG, wonach im Zusammenhang mit der Verletzung von Rechten und/oder Rechtsgütern beim Betrieb eines PKW mit hoch- oder vollautomatisierter Fahrfunktion die durch ein Satellitennavigationssystem ermittelten und in einem Kraftfahrzeug gespeicherten Positions- und Zeitangaben in anonymisierter Form zu Zwecken der Unfallforschung an Dritte übermittelt werden können. Diese Norm verpflichtet den Halter des PKW und betrifft anonymisierte Daten, weshalb eine datenschutzrechtliche Erlaubnisnorm zur Datenzugangsverschaffung nicht erforderlich ist. Die Norm hätte daher für den Fall, dass sie lediglich eine Erlaubnis der Datenzugangsgewährung normieren würde, keinen Anwendungsbereich. Aus dem Verhältnis zu § 63a Abs. 3 StVG, in dem ein solcher Anspruch explizit normiert ist, lässt sich wiederum eher auf eine bloße Erlaubnis der Datenzugangsgewährung schließen. Der Gesetzgeber sollte hier klarstellen, welchen Charakter er § 63a Abs. 5 StVG beimessen möchte. Methodisch muss bis zu einer solchen Klarstellung von einer Erlaubnis der Datenzugangsgewährung ausgegangen werden. Aufgrund der verbleibenden

[154] Vgl. auch die Regelungen aus anderen Bundesländern in den § 45 LKHG BW; Art. 24 Abs. 2 BayKrG; § 28 BbgKHEG; § 2 BremKHDSG; § 8 HmbKHG; §§ 10, 13 GDSG NW; § 13 SKHG; § 16 KHG LSA.

Rechtsunsicherheit wird aber § 63a StVG in die nachfolgende Untersuchung der echten Forschungsklauseln mit eingestellt.

- § 1g Abs. 5 StVG, wonach das Kraftfahrt-Bundesamt berechtigt ist, bestimmte beim Halter erhobene Daten, soweit sie in nicht personenbezogener Form vorliegen, für verkehrsbezogene Gemeinwohlzwecke, insb. zum Zweck der wissenschaftlichen Forschung im Bereich der Digitalisierung, Automatisierung und Vernetzung sowie zum Zweck der Unfallforschung im Straßenverkehr, bestimmten Stellen zugänglich zu machen. Die Gesetzesbegründung führt in Bezug auf § 1g Abs.5 StVG aus:

> *„Besonders im Hinblick auf die Anfangsphase des Betriebes ist daher die Übertragung und Verarbeitung von Daten aus automatisierten und autonomen Systemen in Kraftfahrzeugen zu regeln**. Darüber hinaus** ist es jedoch auch wichtig, die Daten in nicht-personenbezogener Form für Gemeinwohlzwecke, namentlich die wissenschaftliche Forschung im Bereich Digitalisierung, Automatisierung und Vernetzung sowie die Unfallforschung im Straßenverkehr **nutzbar zu machen**."*[155]

Deutlicher ist noch die Gesetzesbegründung in der Fassung vom 8.2.2021, wo es heißt:

> *„Absatz 5 ergänzt die Berechtigung des Kraftfahrt-Bundesamts und stellt einen **Datenzugang** zu nichtpersonenbezogenen Daten gemäß Absatz 1 für verkehrsbezogene Gemeinwohlzwecke sicher, die im Rahmen des autonomen Fahrens ohnehin anfallen."*[156]

§ 1g Abs. 5 StVG muss daher im Ergebnis ein Doppelcharakter beigemessen werden. Auch er ist in der nachfolgenden Untersuchung der echten Forschungsklauseln insofern zu berücksichtigen.

[155] BT-Drs. 19/27439, S. 26; Hervorhebung durch die Verfasserin.
[156] Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes, des Pflichtversicherungsgesetzes und des Gesetzes zum autonomen Fahren, Bearbeitungsstand v. 08.02.2021, S. 43, abrufbar unter https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes-fahren.pdf?__blob=publicationFile, zuletzt abgerufen am 20.07.2021.

Übersicht: Regulierungsstruktur und gesetzliche Grundlagen eines Forschungsdatenzugangs

Echte Forschungsklauseln				Erlaubnisse der Datenzugangsgewährung	
Echte Forschungsklauseln mit Wirkung gegen private Unternehmen		Echte Forschungsklauseln mit Wirkung gegen öffentliche Stellen		Zugang zu personenbezogenen Daten	Zugang zu nicht-personenbezogenen Daten
Abgeleitete Datenzugangs-ansprüche	Originäre Datenzugangs-ansprüche	Gebundene Ansprüche	Ansprüche auf ermessens-fehlerfreie Entscheidung		
§ 19 Abs. 3 UrhDaG	§ 5a NetzDG	§ 303e Abs. 1, Abs. 3 SGB V	Art. 3 VO 557/2013	§ 27 BDSG	§ 63a Abs. 5 StVG
	Art. 31 DSA-E	§ 10 BArchG	§ 8 Abs. 1 KrebsregisterG-E	§ 476 StPO	§ 1g Abs. 5 StVG
		Landesarchivgesetze	§ 8 Abs. 6 KrebsregisterG-E	§ 186 StVollzG i.V.m. § 476 StPO	
		§ 32 StUG	§ 13 BayKRegG	§ 98 SGB XI	
			§ 363 Abs. 3 i.V.m. § 303e Abs. 2 Nr. 7, 8 SGB V	§ 119 SGB XII	
			§ 150b GewO	§ 42a BZRG	
			§ 66 PStG	§ 75 SGB X	
			§ 16 Abs. 6 BStatG	§ 67c Abs. 5 SGB X	
			§ 15 Abs. 4 LStatG BW	§ 14 Abs. 2a, § 15 TPG	
			§ 303e Abs. 4 SGB V	§ 24a Abs. 1 AZRG	
			§ 1g Abs. 5 StVG	§ 34 SächsKHG	
				§ 35 Abs. 7 HMG	
				§ 88a Abs. 4 AufenthaltsG	

VIII. Analyse der nationalen Forschungsklauseln

Ausgehend von dieser Regulierungsstruktur und dem Ziel dieses Gutachtens folgend, einen privilegierten Zugang zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln zu gewährleisten, sind nachfolgend sämtliche echte Forschungsklauseln im Hinblick auf ihren Anwendungsbereich, die Anspruchsberechtigung, die Antragsvoraussetzungen, die Voraussetzungen für die Zugänglichmachung, ihre Schranken, die Beweislastverteilung, die Vergütungsregelung, die Frist, innerhalb der der Datenzugang zu gewähren ist, sowie die Rechtsdurchsetzungsmöglichkeiten und die institutionelle Einbindung in mögliche Datentreuhandstrukturen zu analysieren. Die Erlaubnisse der Datenzugangsgewährung begründen hingegen keinen eigenständigen Anspruch auf Datenzugang und haben daher für die folgenden Untersuchungen Relevanz einzig mit Blick auf die ggf. in die jeweiligen Forschungsklauseln zu integrierende datenschutzrechtliche Verarbeitungsgrundlage. In die Einzelanalyse werden sie daher nicht eingestellt.

1. Anwendungsbereich

a) Ergebnisse

Mit Blick auf den Anwendungsbereich lassen sich insgesamt drei Erkenntnisse aus den existenten Datenzugangsansprüchen ziehen:

1. Forschungsklauseln existieren de lege lata in den Sektoren Online-Wirtschaft, Gesundheit und Mobilität, nicht aber im Energiesektor. Die Forschungsklauseln im Bereich Archivwesen/Verwaltung kommen hinzu, die in Anbetracht des Untersuchungsgegenstands (Forschungsdatenzugang in den Sektoren Online-Wirtschaft, Gesundheit, Mobilität und Energie) aber nicht vertieft werden.

2. Es lässt sich insgesamt ein sehr enger Anwendungsbereich der existenten Datenzugangsansprüche beobachten, der zweifach spezifiziert ist, nämlich erstens mit Blick auf die erfassten Daten und zweitens mit Blick auf die Zugangsadressaten. Es existiert kein sektorübergreifender Datenzugangsanspruch für Forschung und Wissenschaft, sondern wenige und zudem äußerst beschränkte sektorspezifische Datenzugangsansprüche.

3. Datenzugangsansprüche werden über alle Sektoren hinweg regelmäßig gewährleistet aufgrund eines Gemeinwohlinteresses an den betroffenen Daten.

4. Sind Datenzugangsansprüche gegen öffentlich-rechtliche Stellen gerichtet existiert ein Ermessensspielraum des Zugangsadressaten jedenfalls im Gesundheitssektor umso eher, je größer das Risiko des Datenzugangs für das informationelle Selbstbestimmungsrecht des von der Datenverarbeitung Betroffenen ausfällt. Je höher die Schutzvorkehrungen z.B. durch

Anonymisierungslösungen ausfallen, desto eher kommt es in der Rechtsfolge zu einer gebundenen Entscheidung. Eine solche gebundene Entscheidung ist aus Sicht der Forschung zu bevorzugen.[157] Die Schutzvorkehrungen sollten insofern entsprechend hoch ausfallen, um eine gebundene Entscheidung rechtfertigen zu können. Im Mobilitätssektor hingegen besteht ein Ermessen auch im Falle des Zugangs zu nicht-personenbezogenen Daten.

b) Übersicht

Forschungsklausel	Sektor	Erfasste Daten	Zugangsadressat
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	Daten über den Einsatz von Verfahren zur automatisierten und nicht automatisierten Erkennung und Blockierung von Inhalten	Diensteanbieter i.S.d. § 2 UrhDaG
§ 5a NetzDG	Online-Wirtschaft	Qualifizierte Auskunft über: - den Einsatz und die konkrete Wirkweise von Verfahren zur automatisierten Erkennung von Inhalten, die entfernt oder gesperrt werden sollen, insb. zu Art und Umfang eingesetzter Technologien und den Zwecken, Kriterien und Parametern für deren Programmierung sowie zu den eingesetzten Daten, - die Verbreitung von Inhalten, die Gegenstand von Beschwerden über rechtswidrige Inhalte waren oder die vom Anbieter entfernt oder gesperrt worden sind, insb. die entsprechenden Inhalte sowie Informationen darüber, welche Nutzer in welcher Weise mit den Inhalten interagiert haben.	Anbieter eines sozialen Netzwerkes i.S.d. § 1 Abs. 1 NetzDG
Art. 31 DSA-E	Online-Wirtschaft	Daten zum ausschließlichen Zweck der Durchführung von Forschungsarbeiten, die zur Ermittlung und zum Verständnis „systemischer Risiken“ gemäß Art. 26 Abs. 1 beitragen.	Sehr große Online-Plattformen i.S.d.
§ 303e Abs. 1, Abs. 3 S. 1-3 SGB V	Gesundheit	Vom Spitzenverband Bund der Krankenkassen und von der Vertrauensstelle an das	Forschungsdaten-zentrum

[157] So auch: *Havel*, Informationszugangsansprüche des forschenden Wissenschaftlers, S. 453.

		Forschungsdatenzentrum übermittelte Daten in anonymisierter und aggregierter Form	
§ 303e Abs. 3 S. 4 SGB V	Gesundheit	Vom Spitzenverband Bund der Krankenkassen und von der Vertrauensstelle an das Forschungsdatenzentrum übermittelte Daten in anonymisierter und aggregierter Form	Forschungsdaten-zentrum
§ 303e Abs. 4 SGB V	Gesundheit	Vom Spitzenverband Bund der Krankenkassen und von der Vertrauensstelle an das Forschungsdatenzentrum übermittelte Daten mit kleinen Fallzahlen in pseudonymisierter Form	Forschungsdaten-zentrum
§ 8 Abs. 1 KrebsregisterG-E	Gesundheit	Im Krebsregister gespeicherte Daten sowie aggregierte Daten	Zentrum für Krebsregisterdaten beim Robert Koch-Institut
§ 8 Abs. 6 KrebsregisterG-E	Gesundheit	Pseudonymisierte Einzeldatensätze	Zentrum für Krebsregisterdaten beim Robert Koch-Institut
§ 13 Abs. 1 S. 1 BayKRegG	Gesundheit	Im Krebsregister gespeicherte anonymisierte Daten	Landeskrebsre-gister
§ 13 Abs. 1 S. 2 BayKRegG	Gesundheit	Im Krebsregister gespeicherte pseudonymisierte und personenidentifizierende Daten	Landeskrebsre-gister
§ 363 Abs. 4 i.V.m. § 303e Abs. 2 Nr. 7, 8 SGB V	Gesundheit	Daten aus der elektronischen Patientenakte	Forschungsdatenze ntrum
§ 1g Abs. 5 StVG	Mobilität	1. Fahrzeugidentifizierungsnummer 2. Positionsdaten 3. Anzahl und Zeiten der Nutzung sowie der Aktivierung und der Deaktivierung der autonomen Fahrfunktion 4. Anzahl und Zeiten der Freigabe von alternativen Fahrmanövern 5. Systemüberwachungsdaten einschließlich Daten zum Softwarestand 6. Umwelt- und Wetterbedingungen 7. Vernetzungsparameter wie beispielsweise Übertragungslatenz und verfügbare Bandbreite 8. Name der aktivierten und deaktivierten passiven und aktiven	Kraftfahrt-Bundesamt

		Sicherheitssysteme, Daten zum Zustand dieser Sicherheitssysteme sowie die Instanz, die das Sicherheitssystem ausgelöst hat, 9. Fahrzeugbeschleunigung in Längs- und Querrichtung 10. Geschwindigkeit 11. Status der lichttechnischen Einrichtungen 12. Spannungsversorgung des Kraftfahrzeugs mit autonomer Fahrfunktion 13. von extern an das Kraftfahrzeug gesendete Befehle und Informationen. 14. Vor- und Nachname der als Technische Aufsicht eingesetzten Person sowie Nachweise über ihre fachliche Qualifikation	
§ 63a Abs. 5 StVG		Durch ein Satellitennavigationssystem ermittelte Positions- und Zeitangaben, wann ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und einem hoch- oder vollautomatisierten System erfolgt sowie solche Daten, die gespeichert werden, wenn der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische Störung des Systems auftritt	Fahrzeughalter

c) Erläuterungen

aa) Online-Wirtschaftssektor

Nach § 19 Abs. 3 UrhDaG haben Diensteanbieter zum Teilen von Online-Inhalten gem. § 2 UrhDaG Zugang zu Daten über den Einsatz von Verfahren zur automatisierten und nicht automatisierten Erkennung und Blockierung von Inhalten zu gewähren. Hieraus sollen Erkenntnisse über die Art der von den Diensteanbietern ergriffenen Maßnahmen zur automatisierten Erkennung und Blockierung von Inhalten gewonnen werden können. Zugang ist ausweislich der Gesetzesbegründung zu gewähren zu Daten über die eingesetzten Filtertechnologien sowie die Art der Inhalte, die über diese Filtertechnologien erkannt und gegebenenfalls blockiert werden. Die Forschung mit solchen Daten aus dem Plattformumfeld soll insb. Aufschluss über die teils wenig transparenten Selektions- und Ordnungsleistungen von Algorithmen schaffen, die auf Plattformen zum Einsatz kommen.[158] Der Datenzugangsanspruch soll also die Erforschung von Fragen von besonderem öffentlichen Interesse

[158] BT-Drs. 19/29894, S. 100.

ermöglichen, denn die urheberrechtlichen Schrankenbestimmungen, die durch Filtertechniken eingeschränkt werden könnten, dienen in nicht unerheblichem Maße den Kommunikationsgrundrechten, die nicht hinter dem Schutz des Urhebers zurückstehen dürfen.[159]
Nach § 5a NetzDG kann ein Forscher vom Anbieter eines sozialen Netzwerkes qualifizierte Auskünfte verlangen über:

1. den Einsatz und die konkrete Wirkweise von Verfahren zur automatisierten Erkennung von Inhalten, die entfernt oder gesperrt werden sollen, insb. zu Art und Umfang eingesetzter Technologien und den Zwecken, Kriterien und Parametern für deren Programmierung sowie zu den eingesetzten Daten,

2. die Verbreitung von Inhalten, die Gegenstand von Beschwerden über rechtswidrige Inhalte waren oder die vom Anbieter entfernt oder gesperrt worden sind, insb. die entsprechenden Inhalte sowie Informationen darüber, welche Nutzer in welcher Weise mit den Inhalten interagiert haben.

Nach der Gesetzesbegründung ist § 5a explizit auf soziale Netzwerke beschränkt. Eine Ausweitung des Anspruchs auf Videosharingplattform-Dienste nach § 3e Abs. 2 NetzDG findet nicht statt. Die von der Forschungsklausel erfassten Daten betreffen mit der Funktionsweise von Plattformen und dem dortigen Prozess der Inhalteverbreitung Fragen von erheblichem öffentlichem Interesse, da der für eine Demokratie essentielle Meinungsbildungsprozess der Bevölkerung zunehmend auf diesen Plattformen stattfindet.[160] Qualifizierte Auskünfte sind unverfälschte, beim Anbieter des sozialen Netzwerkes vorliegende Daten, aber auch dort aufbereitete Informationen, etwa Erkenntnisse aus vom Anbieter vorgenommenen Auswertungen der beim Anbieter vorliegenden Daten.[161]

Die Forschungsklausel des Art. 31 DSA-E gewährleistet einen Anspruch auf Datenzugang gegen sehr große Online-Plattformen. ErwGr. 54 DSA-E definiert sehr große Online-Plattformen als solche Plattformen, deren Nutzerzahl eine operative Schwelle von 45 Millionen überschreitet, wobei die operative Schwelle durch Änderungen im Wege delegierter Rechtsakte aktualisiert werden können soll, soweit dies erforderlich ist. Grund der stärkeren Regulierung solcher sehr großer Online-Plattformen sind die gesellschaftlichen Risiken, die ihr Betrieb nach sich ziehen kann und die sich hinsichtlich Umfang und Auswirkungen von denen kleinerer Plattformen unterscheiden. Solche sehr großen Online-Plattformen sollen höheren Sorgfaltspflichten unterliegen, die in einem angemessenen

[159] Siehe zuletzt: EuGH, Urteil v. 22.06.2021 - C-682/18 und C-683/18 = ECLI:EU:C:2021:503 (Youtube), Rn. 135; Schlussanträge des Generalanwalts v. 15.07.2021, C-401/19.
[160] BT-Drs. 19/29392, S. 18; *Klaus*/*Meyer*, Regulierung digitaler Kommunikationsplattformen, Böll Brief, 2021, abrufbar unter: https://www.boell.de/sites/default/files/2021-06/böll.brief%20G14%20Regulierung%20digitaler%20Kommunikation%20splattformen.pdf, zuletzt abgerufen am 16.07.2021.
[161] BT-Drs. 19/29392, S. 20.

Verhältnis zu ihren gesellschaftlichen Auswirkungen und Mitteln stehen. Der DSA-E verfolgt damit einen risikobasierten Ansatz. Die Art und Weise, in der sehr große Online-Plattformen genutzt werden, hat großen Einfluss auf die Online-Sicherheit, die öffentliche Meinungsbildung und den öffentlichen Diskurs sowie den Online-Handel.[162]

Vom Datenzugangsanspruch umfasst sind Daten zum ausschließlichen Zweck der Durchführung von Forschungsarbeiten, die zur Ermittlung und zum Verständnis systemischer Risiken gemäß Art. 26 Abs. 1 dienen. Nach ErwGr. 64 zählen dazu beispielsweise Daten, die erforderlich sind, um die mit den Systemen der Plattform verbundenen Risiken und möglichen Schäden zu bewerten, sowie Daten zur Genauigkeit, Funktionsweise und Prüfung von Algorithmensystemen für die Moderation von Inhalten, Empfehlungs- oder Werbesysteme oder Daten zu Verfahren und Ergebnissen der Moderation von Inhalten oder von internen Beschwerdemanagementsystemen im Sinne dieser Verordnung.

Systemische Risiken sind gem. ErwGr. 57 DSA-E in drei Kategorien zu unterscheiden:
Erstens, Risiken, die durch einen Missbrauch des Dienstes durch Verbreitung illegaler Inhalte entstehen können, darunter die Verbreitung von Material über sexuellen Kindesmissbrauch oder von illegaler Hassrede sowie illegale Tätigkeiten wie ein nach Unions- oder nationalem Recht untersagter Verkauf von Waren oder Dienstleistungen, wie z.B. nachgeahmter Güter. Ein ganz erhebliches systemisches Risiko entsteht, wenn der Zugang zu diesen Inhalten durch Konten mit einer besonders großen Reichweite verstärkt werden kann. Eine zweite Risikokategorie stellen die Auswirkungen des Dienstes auf die Ausübung der durch die Charta der Grundrechte geschützten Grundrechte, einschließlich der Freiheit der Meinungsäußerung und der Informationsfreiheit, des Rechts auf Achtung des Privatlebens, des Rechts auf Nichtdiskriminierung und der Rechte des Kindes dar. Diese Risiken können beispielsweise auf die Gestaltung der Algorithmensysteme sehr großer Online-Plattformen oder auf den Missbrauch ihres Dienstes für die Übermittlung missbräuchlicher Nachrichten oder auf andere Methoden zur Verhinderung der freien Meinungsäußerung oder zur Behinderung des Wettbewerbs zurückzuführen sein. Eine dritte Kategorie von Risiken betrifft die absichtliche und oftmals auch koordinierte Manipulation des Dienstes der Plattform, die absehbare Auswirkungen auf Gesundheit, den gesellschaftlichen Diskurs, Wahlprozesse, die öffentliche Sicherheit und den Schutz Minderjähriger haben kann. Solche Risiken können beispielsweise auf die Einrichtung von Scheinkonten, die Nutzung von Bots und anderen automatisierten oder teilautomatisierten Verhaltensweisen zurückzuführen sein, die zu einer schnellen und umfangreichen Verbreitung von Informationen führen können, die illegale Inhalte darstellen oder mit den Geschäftsbedingungen einer

[162] ErwGr. 56 DSA-E.

Online-Plattform unvereinbar sind.[163] Es geht also auch hier um die Gewährleistung bzw. Beeinträchtigung von Grundrechten und damit bereits generell um eine besonders im öffentlichen Interesse stehende Frage, die durch den Datenzugang von Wissenschaft und Forschung besser untersucht werden können soll.

bb) Gesundheitssektor

Das Forschungsdatenzentrum macht nach § 303e Abs. 1 SGB V die ihm vom Spitzenverband Bund der Krankenkassen und von der Vertrauensstelle an das Forschungsdatenzentrum übermittelten Daten für Forschung und Wissenschaft zugänglich. Ist der Antrag entsprechend gestellt, hat das Forschungsdatenzentrum keinen Ermessensspielraum.[164] Ein solcher besteht aber in zwei spezifischen Fällen, nämlich nach § 303e Abs. 3 S. 4 SGB V erstens dann, wenn Daten für kleine Fallzahlen angefordert werden, die das Risiko einer Identifikation von Versicherten und den sie behandelnden Leistungserbringern in sich tragen, z.B. im Falle einer seltenen Erkrankung durch Ärzte einer bestimmten Fachrichtung in einer ausgewählten Region,[165] und nach § 303e Abs. 4 SGB V zweitens dann, wenn die Nutzung pseudonymisierter Einzeldatensätze für die Durchführung eines Forschungsvorhabens erforderlich und dies für das Forschungsdatenzentrum nach Maßgabe des Antrags nachvollziehbar ist. Es bestehen allerdings Zweifel an der Verfassungsmäßigkeit der Regelung des § 303e Abs. 4 SGB V.[166] U.a. empfahl der Bundesrat eine Überarbeitung der Regelung unter sozialdatenschutzrechtlichen Gesichtspunkten und begründete dies mit Zweifeln an der Verhältnismäßigkeit der antragsgegenständlichen Normen im Hinblick auf die Persönlichkeitsrechte der Betroffenen.[167] Auch im Rahmen einer Sachverständigenanhörung im Bundestag wurden aus diesem Grund Zweifel an der Verfassungsmäßigkeit der Vorschrift geäußert.[168]

Die Einrichtung eines Forschungsdatenzentrums basiert auf dem Digitale-Versorgung-Gesetz. Wesentliche Funktionseinheiten der ehemaligen Datenaufbereitungsstelle beim Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) und das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), das das Forschungsdatenzentrum verantwortet, wurden zusammengeführt.[169] Die Patientendaten werden von den Krankenkassen an den GKV-Spitzenverband weitergeleitet, der sie wiederum an das neue Zentrum übergibt. Eine beim Robert Koch-Institut

[163] ErwGr. 57 DSA-E.
[164] *Hess*, in: Körner/Mutschler/Leitherer/Rolfs, Kasseler Kommentar Sozialversicherungsrecht, 112. Ergänzungslieferung, 2020, § 303e Rn. 13.
[165] *Hess*, in: Körner/Mutschler/Leitherer/Rolfs, Kasseler Kommentar Sozialversicherungsrecht, 112. Ergänzungslieferung, 2020, § 303e Rn. 13.
[166] Siehe aber BVerfG, Beschluss vom 19.3.2020 – 1 BvQ 1/20; *Hess*, in: Körner/Mutschler/Leitherer/Rolfs, Kasseler Kommentar Sozialversicherungsrecht, 112. Ergänzungslieferung, 2020, § 303e Rn. 14; BT-Drs. 17/6909 zu Art. 1 Nr. 83.
[167] Vgl. BRDrucks 360/19, S. 8-9.
[168] BT-Ausschussprotokoll 19/63, S. 17 ff.
[169] https://www.dimdi.de/dynamic/de/das-dimdi/aktuelles/meldung/bundesinstitut-fuer-arzneimittel-und-medizinprodukte-und-wesentliche-funktionseinheiten-des-dimdi-zusammengefuehrt/, zuletzt abgerufen am 16.07.2021.

angesiedelte Vertrauensstelle soll die Pseudonymisierung gewährleisten.[170] Auch Daten aus der elektronischen Patientenakte sollen pseudonymisiert an das Forschungsdatenzentrum übermittelt werden. Auch im Hinblick auf diese Daten besteht ein Zugangsanspruch von Wissenschaft und Forschung.[171]

cc) Mobilitätssektor

§ 1g Abs. 5 StVG soll einen Zugangsanspruch zu Daten, die beim autonomen Fahren anfallen, für verkehrsbezogene Gemeinwohlzwecke sicherstellen.[172] Er soll allein nicht-personenbezogene Daten betreffen.[173] § 63a Abs. 5 StVG hingegen betrifft die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben, wann ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und einem hoch- oder vollautomatisierten System erfolgt sowie solche Daten, die gespeichert werden, wenn der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische Störung des Systems auftritt. Regelungsadressat ist der Fahrzeughalter, was stark kritisiert wird.[174] Denn der Fahrzeughalter hat keine Möglichkeit, die Übermittlung der Daten zu veranlassen, weil er technisch nicht die Kontrolle über die Daten und rechtlich nicht die Befugnis hat, auf die Daten zuzugreifen.

> *„Allerdings drängt sich sogleich die Frage auf, wie der Halter seiner damit einhergehenden Pflicht nachkommen soll, wenn er weder Zugriff auf die Mobilitätsdaten der Blackbox noch einen eigenen Auskunftsanspruch gegen den Hersteller hat oder die Daten – abhängig von dem noch durch Rechtsverordnung festzulegenden Speicherort – außerhalb des Fahrzeugs auf einem Server des Herstellers abgelegt werden."*[175]

Es handelt sich faktisch um eine Norm ohne Adressaten.[176] Daraus erklärt sich auch, weshalb

> *[e]ine Übermittlung der gemäß § 63a Abs. 1 StVG gespeicherten Daten an Dritte im Sinne des § 63a Abs. 5 StVG [...] derzeit nicht statt [findet].*[177]

---

[170] https://www.gerechte-gesundheit.de/news/detail/forschungsdatenzentrum-nimmt-form-an.html, zuletzt abgerufen am 16.07.2021.
[171] *Hess*, in: Körner/Mutschler/Leitherer/Rolfs, Kasseler Kommentar Sozialversicherungsrecht, 112. Ergänzungslieferung, 2020, § 303e Rn. 14-21.
[172] Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes–Gesetz zum autonomen Fahren, Bearbeitungsstand 8.2.2021, S. 43, abrufbar unter https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes-fahren.pdf?__blob=publicationFile, zuletzt abgerufen am 20.07.2021.
[173] BT-Drs. 19/27439, S. 26.
[174] *Hoeren*, Ein Treuhandmodell für Autodaten? – § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion, NZV 2018, 153, 154; *Wagner*/*Goebele*, Freie Fahrt für das Auto der Zukunft?, ZD 2017, 263, 268.
[175] *Von Bodungen*, in: Specht/Mantz, Handbuch deutsches und europäisches Datenschutzrecht, § 16 Rn. 57.
[176] *Hoeren*, Ein Treuhandmodell für Autodaten? – § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion, NZV 2018, 153, 154.
[177] BT-Drs. 19/9544, S. 3.

Der Arbeitskreis II des Verkehrsgerichtstags 2018 hat daher die Einbindung in eine Datentreuhandstruktur empfohlen, wobei auch hier der Fahrzeughalter der Datenzugangsadressat bleiben soll.[178]

2. Anspruchsberechtigung

a) Ergebnisse

Die Forschungsklauseln weisen in der Regel „Forschung und Wissenschaft", spezifische Forschungseinrichtungen oder spezifische Wissenschaftler als Anspruchsberechtigte aus. Welche Anforderungen an die anspruchsberechtigen Einrichtungen und Personen zu stellen sind, wird z.T. durch den Gesetzestext, z.T. durch die Gesetzesbegründung spezifiziert. Z.T. fehlt eine Spezifizierung auch gänzlich. Relevant ist insb. die Frage, ob die de lege lata existenten Forschungsklauseln auch zugunsten der kommerziellen Forschung ausgestaltet sind und falls ja, was hierunter zu verstehen ist. Es lassen sich insgesamt folgende Erkenntnisse festhalten:

1. Der kommerzielle Charakter wissenschaftlicher Forschung führt nicht normübergreifend zu einem Ausschluss der Anspruchsberechtigung.

2. Viele – jedoch nicht sämtliche – Forschungsklauseln fordern eine im öffentlichen Interesse, z.T. auch eine im Gemeinwohlinteresse liegende Forschung.

3. Die Erkenntnisse aus den Forschungsklauseln im Hinblick auf die Zugangsadressaten lassen sich grundrechtsdogmatisch erklären: Das Gemeinwohlinteresse ist ein besonders schwerwiegendes öffentliches Interesse und ist daher grundrechtsdogmatisch besonders geeignet, um die mit einem Forschungsdatenzugang verbundenen Eingriffe in die Grundrechte der Zugangsadressaten zu rechtfertigen. Je eher das Gemeinwohlinteresse auch durch kommerzielle Forschung erreicht werden kann, desto eher lässt sich auch diese über die Forschungsklauseln als anspruchsberechtigt erfassen.

b) Übersicht

Forschungsklausel	Sektor	Antragsberechtigte
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	Berechtigte i.S.d. § 60d Abs. 2 UrhG
§ 5a NetzDG	Online-Wirtschaft	Forscher
Art. 31 DSA-E	Online-Wirtschaft	Zugelassene Forscher
§ 303e Abs. 1, Abs. 3 S. 1-3 SGB V	Gesundheit	Institutionen der Gesundheitsversorgungsforschung, Hochschulen, die nach landesrechtlichen

[178] *Specht-Riemenschneider*/*Blankertz* et al., Die Datentreuhand, MMR-Beilage 2021, S. 25, 25; *Hoeren*, Ein Treuhandmodell für Autodaten? – § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion, NZV 2018, 153, 154.

		Vorschriften anerkannten Hochschulkliniken, öffentlich geförderte außeruniversitäre Forschungseinrichtungen und sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, sofern die Daten wissenschaftlichen Vorhaben dienen
§ 303e Abs. 3 S. 4 SGB V	Gesundheit	Institutionen der Gesundheitsversorgungsforschung, Hochschulen, die nach landesrechtlichen Vorschriften anerkannten Hochschulkliniken, öffentlich geförderte außeruniversitäre Forschungseinrichtungen und sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, sofern die Daten wissenschaftlichen Vorhaben dienen
§ 303e Abs. 4 SGB V	Gesundheit	Institutionen der Gesundheitsversorgungsforschung, Hochschulen, die nach landesrechtlichen Vorschriften anerkannten Hochschulkliniken, öffentlich geförderte außeruniversitäre Forschungseinrichtungen und sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, sofern die Daten wissenschaftlichen Vorhaben dienen
§ 8 Abs. 1 KrebsregisterG-E § 8 Abs. 6 KrebsregisterG-E	Gesundheit	Öffentliche und private Einrichtungen und Personen
§ 13 Abs. 1 S. 1 BayKRegG § 13 Abs. 1 S. 2 BayKRegG	Gesundheit	Dritte mit wissenschaftlichem Interesse
§ 1g Abs. 5 StVG	Mobilität	Hochschulen und Universitäten, außeruniversitäre Forschungseinrichtungen, Bundes-, Landes- und Kommunalbehörden mit Forschungs-, Entwicklungs-, Verkehrsplanungs- und Stadtplanungsaufgaben
§ 63a Abs. 5 StVG	Mobilität	Dritte

c) Erläuterungen

aa) Online-Wirtschaftssektor

(1) § 19 Abs. 3 UrhDaG

§ 19 Abs. 3 UrhDaG verweist für die Anspruchsberechtigung auf § 60d Abs. 2 UrhG. Berechtigt sind danach Forschungsorganisationen (einschließlich der der ihnen angehörenden Forschenden[179]). Forschungsorganisationen sind Hochschulen, Forschungsinstitute oder sonstige Einrichtungen, die wissenschaftliche Forschung betreiben, sofern sie

1. nicht kommerzielle Zwecke verfolgen

2. sämtliche Gewinne in die wissenschaftliche Forschung reinvestieren oder

3. im Rahmen eines staatlich anerkannten Auftrags im öffentlichen Interesse tätig sind.

Diese Legaldefinition entspricht der Vorgabe aus Artikel 2 Nummer 1 DSM-RL. Die Formulierung soll lediglich „gestrafft" sein, ohne dass der Aussagegehalt des Artikels 2 Nummer 1 DSM-RL verändert werden sollte.[180] Der Begriff der wissenschaftlichen Forschung ist aufgrund des unionsrechtlichen Hintergrunds der Regelung autonom unionsrechtlich auszulegen. Auf Vorgaben aus § 60d UrhG a.F., der auf das Urheberrechtswissensgesellschaftsgesetz zurückzuführen ist, kann nicht zurückgegriffen werden.[181] Wissenschaftliche Forschung erfordert daher eine Tätigkeit mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen (s.o.). Der Kreis der Anspruchsberechtigten wird im Sinne der Nr. 1 – 3 beschränkt. Es genügt, dass eines der drei genannten Kriterien erfüllt ist; es können aber auch mehrere oder sämtliche Voraussetzungen erfüllt sein.[182] Kommerzielle Forschung wird daher nicht per se von einer Anspruchsberechtigung ausgeschlossen. Werden sämtliche Gewinne in die wissenschaftliche Forschung reinvestiert oder erfolgt die wissenschaftliche Forschung im Rahmen eines staatlich anerkannten Auftrags im öffentlichen Interesse, so sind auch kommerziell tätige Forschungsorganisationen anspruchsberechtigt.

Kennzeichnend für einen staatlich anerkannten Auftrag im öffentlichen Interesse gemäß § 60d Abs. 2 Satz 1 Nummer 3 UrhG-E sind beispielsweise die Finanzierung durch die öffentliche Hand oder Bestimmungen zum öffentlichen Interesse in Rechtsvorschriften oder in Aufträgen der öffentlichen Hand (vergleiche ErwGr 12 Satz 6 DSM-RL).[183] Nach ErwGr 12 S. 2 DSM-RL bezieht sich wissenschaftliche Forschung sowohl auf die Natur- als auch auf die Geisteswissenschaften. Auch individuelle Nutzer, die einer Forschungsorganisation angehören, fallen nach ErwGr 14 Satz 1 und 3

[179] Formulierungshilfe für einen Änderungsantrag zur Einfügung einer Forschungsklausel in dem Entwurf für ein Urheberrechts-Diensteanbieter-Gesetz, S. 2, abrufbar unter: https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2021&num=38, zuletzt abgerufen am 16.07.2021.
[180] BT-Drs. 19/27426, S. 96.
[181] *Möllers*, Juristische Methodenlehre, 2. Auflage 2019, § 2 Rn. 71-73.
[182] BT-Drs. 19/27426, S. 96.
[183] BT-Drs. 19/27426, S. 96.

DSM-RL unter die Ausnahme für das Text und Data Mining, sofern sie rechtmäßigen Zugang zu den betroffenen Inhalten haben.

Arbeiten Forschungsorganisationen mit einem privaten Unternehmen zusammen, so schließt dies ihre Anspruchsberechtigung ebenfalls nicht von vornherein aus. Im Rahmen derartiger Public Private Partnerships, vergleiche auch ErwGr 11 Satz 2 DSM-RL, sollen sich nach ErwGr 11 Satz 2 und 3 DSM-RL im Grundsatz auch solche Forschungsorganisationen auf die gesetzliche Erlaubnis für Text und Data Mining berufen können, wenn die Infrastruktur eines privaten Unternehmens verwendet wird.[184] Eine Berechtigung besteht jedoch nicht, wenn ein Unternehmen einen bestimmenden Einfluss auf die Forschungsorganisation und einen bevorzugten Zugang zu den Ergebnissen der wissenschaftlichen Forschung hat (vgl. Artikel 2 Nummer 1 DSM-RL). Ein bestimmender Einfluss eines privaten Unternehmens kann beispielsweise vorliegen, wenn es aufgrund der strukturellen Gegebenheiten in seiner Eigenschaft als Anteilseigner Kontrolle ausüben und dadurch einen bevorzugten Zugang zu den Forschungsergebnissen erhalten kann (vgl. ErwGr 12 Satz 7 DSM-RL).[185]

(2) § 5a NetzDG

Forscher i.S.d. § 5a NetzDG ist jede natürliche oder juristische Person, die wissenschaftliche Forschung betreibt. Für die Bestimmung des Forschungsbegriffes ist auf die grundgesetzlichen Vorgaben zurückzugreifen, wobei § 5a Abs. 3 NetzDG den Kreis der Anspruchsberechtigten verengt. Anspruchsberechtigt sind danach allein Forscher, die Vorhaben einer im öffentlichen Interesse liegenden wissenschaftlichen Forschung zu Art, Umfang, Ursachen und Wirkungsweisen öffentlicher Kommunikation in sozialen Netzwerken und den Umgang der Anbieter hiermit betreiben. Ein öffentliches Interesse soll nach der Gesetzesbegründung in der Regel anzunehmen sein bei Forschungsvorhaben von Hochschulen und außeruniversitären Forschungseinrichtungen in Deutschland. Dabei soll der überwiegenden Finanzierung aus öffentlichen Mitteln eine Indizwirkung für die Annahme eines öffentlichen Interesses zukommen. Im Umkehrschluss bedeutet dies, dass im Falle einer Forschung, die zwar an Hochschulen und außeruniversitären Forschungseinrichtungen stattfindet, jedoch privat finanziert wird, nicht bereits eine Indizwirkung dafürspricht, dass das Forschungsvorhaben im öffentlichen Interesse liegt. Dies wird anderweitig darzulegen und ggf. zu beweisen sein. Die Gesetzesbegründung fordert für die Annahme eines öffentlichen Interesses privater wie öffentlich-finanzierter Forschungsvorhaben, dass die Forschungsergebnisse der Öffentlichkeit zugänglich gemacht werden und dass sie letztlich dem Wohl der Allgemeinheit dienen. Für die Annahme eines öffentlichen Interesses kann es auch sprechen, wenn die Forschung zum Erreichen der Gesetzesziele beiträgt. Gegen ein öffentliches Interesse kann sprechen, wenn aufgrund

[184] BT-Drs. 19/27426, S. 96.
[185] BT-Drs. 19/27426, S. 96.

von Abhängigkeiten von einem Auftraggeber im konkreten Einzelfall der Anschein besteht, dass keine unvoreingenommene Forschung betrieben wird. Zudem kann gegen ein öffentliches Interesse sprechen, wenn Anhaltspunkte bestehen, dass eine Ausforschung zu wirtschaftlichen oder politischen Zielen erfolgen soll.[186]

(3) Art. 31 DSA-E

Art. 31 Abs. 2 DSA-E will zugelassenen Forschern über den Koordinator für digitale Dienste am Niederlassungsort oder der Kommission Zugang zu Daten von sehr großen Online-Plattformen (s.o.) zwecks Durchführung von Forschungsarbeiten, die zur Ermittlung und zum Verständnis systemischer Risiken beitragen (s.o.), gewähren. Um zugelassen zu werden, müssen die Forscher nach Art. 31 Abs. 4 DSA-E mit akademischen Einrichtungen verbunden sein, unabhängig von gewerblichen Interessen sein, nachweislich über Sachkenntnis auf den Gebieten verfügen, die mit den untersuchten Risiken oder den diesbezüglichen Forschungsmethoden zusammenhängen, und sich verpflichten und in der Lage sein, die mit jedem Verlangen verbundenen besonderen Anforderungen an die Datensicherheit und die Vertraulichkeit einzuhalten. Einzelheiten sollen nach Art. 31 Abs. 5 DSA-E in delegierten Rechtsakten der Kommission festgelegt werden.

bb) Gesundheitssektor

§ 303e weist in all seinen Forschungsklauseln spezifische Nutzungsberechtigte als anspruchsberechtigt aus. Im Bereich von Forschung und Wissenschaft sind dies nach § 303e Abs. 1 Nr. 7 und 8 Institutionen der Gesundheitsversorgungsforschung, Hochschulen, die nach landesrechtlichen Vorschriften anerkannten Hochschulkliniken, öffentlich geförderte außeruniversitäre Forschungseinrichtungen und sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, sofern die Daten wissenschaftlichen Vorhaben dienen. Zu den außeruniversitären Forschungseinrichtungen gehören Einrichtungen der Fraunhofer Gesellschaft, der Helmholtz Gemeinschaft, der Leibniz Gemeinschaft sowie der Max-Planck Gesellschaft.[187]

§ 8 KrebsregisterG-E weist als Antragsberechtigte sowohl öffentliche als auch private Einrichtungen und Personen aus. Insb. ist auch die privat finanzierte Forschung erfasst.[188] Noch weiter ist die Formulierung des § 13 BayKrG, die jeden Dritten mit wissenschaftlichem Interesse als antragsberechtigt ausweist.

cc) Mobilitätssektor

[186] BT-Drs. 19/29392, S. 19.
[187] *Hess*, in: Körner/Mutschler/Leitherer/Rolfs, Kasseler Kommentar Sozialversicherungsrecht, 112. Ergänzungslieferung, 2020, § 303e SGB V Rn. 11.
[188] BT-Drs. 19/28185, S. 43.

Die Gesetzesbegründung des § 1g Abs. 5 StVG spezifiziert die Anspruchsberechtigten nicht weiter. Die Forschung muss allerdings verkehrsbezogenen Gemeinwohlzwecken dienen. Inwieweit das kommerzielle Forschungsinteressen ausschließt, wird nicht ausgeführt. Noch weiter geht die Formulierung des § 63a Abs. 5 V StVG, der jeden Dritten als antragsberechtigt erachtet, der Datenzugang zu Zwecken der Unfallforschung begehrt. Unter dem Begriff der Unfallforschung werden Organisationen und Institutionen, die mit dem Ziel der Verhütung zukünftiger Unfälle Ablauf und Ursachen eines Unfalls im Straßenverkehr rekonstruieren, verstanden.[189]

3. Antragsvoraussetzungen

a) Ergebnisse

Hinsichtlich der Antragsvoraussetzungen ist festzuhalten:

1. Zusätzliche Antragsvoraussetzungen werden (mit Ausnahme des Erfordernisses nach nachvollziehbarer Darlegung bestimmter Voraussetzungen, was aber im Wesentlichen eine beweisrechtliche Vorgabe sein dürfte) nur von wenigen Forschungsklauseln vorgegeben. Wo sie aber vorgesehen sind, dienen sie dem Schutz der Grundrechte und Grundfreiheiten Dritter oder des Zugangsadressaten.

2. Ein bei Antragstellung vorzulegendes Schutzkonzept hat höhere Anforderungen zu erfüllen, je höher die durch den Datenzugang entstehenden Risiken für die Grundrechte des Zugangsadressaten oder Dritte ausfällt. Schutzkonzepte sind daher auch und gerade im Interesse von Forschung und Wissenschaft unbedingt zu empfehlen. Denn je geringer die Risiken für die Rechte und Interessen der von einem Datenzugang Betroffenen ausfallen, desto weiter darf der Datenzugangsanspruch im Sinne des Five Safes Models reichen.

b) Übersicht

Forschungsklausel	Sektor	Antragsvoraussetzungen
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	keine
§ 5a NetzDG	Online-Wirtschaft	Vorlage eines Schutzkonzeptes mit folgendem Inhalt: 1. eine Beschreibung der für die Forschungszwecke nach Abs. 3 erforderlichen Informationen 2. eine Beschreibung der beabsichtigten Verwendung der Informationen 3. eine Beschreibung der Vorkehrungen, um eine anderweitige Verwendung der Informationen zu verhindern

[189] BT-Drs. 19/9544, S. 4.

		4. eine Beschreibung der Vorkehrungen, um die schutzwürdigen Interessen des Anbieters zu schützen, und 5. eine Beschreibung der technischen und organisatorischen Maßnahmen, die den Schutz der personenbezogenen Daten sicherstellen.
Art. 31 DSA-E	Online-Wirtschaft	Ist über den Koordinator für digitale Dienste am Niederlassungsort oder der Kommission zu stellen. Dieser hat ein begründetes Verlangen auszusprechen.
§ 303e Abs. 1, Abs. 3 S. 1-3 SGB V	Gesundheit	Nachvollziehbare Darlegung, dass Umfang und Struktur der beantragten Daten geeignet und erforderlich sind, um die zu untersuchende Frage zu beantworten.
§ 303e Abs. 3 S. 4 SGB V	Gesundheit	Nachvollziehbare Darlegung, dass ein nach Abs. 2 zulässiger Nutzungszweck, insb. die Durchführung eines Forschungsvorhabens, die Übermittlung der Daten rechtfertigt.
§ 303e Abs. 4 SGB V	Gesundheit	Nachvollziehbare Darlegung, dass die Nutzung der pseudonymisierten Einzeldatensätze für einen nach § 303e Abs. 2 SGB V zulässigen Forschungszweck, insb. für die Durchführung eines Forschungsvorhabens, erforderlich ist.
§ 8 Abs. 1 KrebsregisterG-E	Gesundheit	Nachvollziehbare Darlegung, dass der Umfang und die Struktur der beantragten Daten geeignet und erforderlich sind, um die zu untersuchenden Fragen zu beantworten und die Angabe des Vorhabens, das mit den beim Zentrum für Krebsregisterdaten vorliegenden Daten bearbeitet werden kann und eine länderübergreifende Auswertung erfordert. Außerdem Darlegung von Zweck und Umfang der Nutzung der beantragten Daten sowie Begründung des methodischen Ansatzes der Datenverarbeitung. Schließlich müssen Angaben zu den an der Datenverarbeitung beteiligten Personen und dazu, ob und ggf. mit welchen anderen Datenbeständen eine Zusammenführung vorgesehen ist, im Antrag enthalten sein.
§ 8 Abs. 6 KrebsregisterG-E	Gesundheit	Nachvollziehbare Darlegung, dass die Bereitstellung pseudonymisierter Einzeldatensätze für die Durchführung des Forschungsvorhabens erforderlich ist.
§ 13 Abs. 1 S. 1 BayKRegG	Gesundheit	Glaubhaftmachung eines berechtigten, insb. wissenschaftlichen Interesses.

§ 13 Abs. 1 S. 2 BayKRegG	Gesundheit	Besondere Begründung, dass pseudonymisierte oder personenbezogene Daten erforderlich sind.
§ 1g Abs. 5 StVG	Mobilität	keine
§ 63a Abs. 5 StVG	Mobilität	keine

c) Erläuterungen

aa) Online-Wirtschaftssektor

Das Schutzkonzept des § 5a NetzDG soll sicherstellen, dass die Belange der von einem Forschungsdatenzugang Drittbetroffenen sowie die Belange des sozialen Netzwerkes ausreichend beachtet werden.[190] Auch dient es der Spezifizierung des geschuldeten Datenzugangs auf die im Schutzkonzept zu beschreibenden Daten. Daneben wird es dem sozialen Netzwerk aber auch die Prüfung der Anspruchsvoraussetzungen und damit der eigenen Datenzugangsverpflichtung ermöglichen. Der Anbieter des sozialen Netzwerkes kann die Auskunft bis zur Vorlage des Schutzkonzeptes verweigern. Das Schutzkonzept ist zugleich der zuständigen Datenschutzaufsichtsbehörde vorzulegen, die bei Anhaltspunkten zu Datenschutzverstößen ein entsprechendes Verfahren einleiten kann.[191]

Der Antrag nach Art. 31 DSA-E ist über den Koordinator für digitale Dienste am Niederlassungsort oder der Kommission zu stellen. Erforderlich ist ein begründetes Verlangen des Koordinators. Der Koordinator für digitale Dienste ist nach Art. 38 Abs. 2 DSA-E eine Behörde, die von und in jedem Mitgliedstaat benannt wird. Er ist grundsätzlich für alle Fragen im Zusammenhang mit der Anwendung und Durchsetzung des Digital Services Act in diesem Mitgliedsstaat zuständig. Gegen eine unberechtigte Verweigerung des begründeten Verlangens nach entsprechendem Antrag an den Koordinator für digitale Dienste wird der Forscher nach nationalem Recht mit einer Verpflichtungsklage vorgehen können, der DSA-E lässt dies ungeregelt (dazu sogleich Unterpunkt Beweislastverteilung). Der Antrag an den Koordinator unterliegt keinen gesetzlich normierten Vorgaben, man wird aber Verlangen müssen, dass er inhaltlich und formal so gefasst ist, dass der Koordinator für digitale Dienste das für den Datenzugangsanspruch erforderliche begründete Verlangen ausdrücken kann. Inwiefern das Verlangen begründet werden muss, lassen Gesetzestext und Erwägungsgründe aber offen.

bb) Gesundheitssektor

[190] Die Gesetzesbegründung sprich insofern lediglich von den „nach § 5a zu berücksichtigenden Gewährleistungen“, vgl. BT-Drs. 19/29392, S. 20.
[191] BT-Drs. 19/29392, S. 20.

Für die Forschungsklauseln des § 303e SGB V erforderlich sind jeweils nachvollziehbare Darlegungen, dass Umfang und Struktur der beantragten Daten geeignet und erforderlich sind, um die zu untersuchende Frage zu beantworten, dass ein nach Abs. 2 zulässiger Nutzungszweck, insb. die Durchführung eines Forschungsvorhabens, die Übermittlung der Daten rechtfertigt bzw. dass die Nutzung der pseudonymisierten Einzeldatensätze für einen nach § 303e Abs. 2 SGB V zulässigen Forschungszweck, insb. für die Durchführung eines Forschungsvorhabens, erforderlich ist. Notwendigerweise geht dies einher mit einer Beschreibung der Datensätze, zu denen Forschungsdatenzugang begehrt wird. Zu erklären sind diese Voraussetzungen des Zugangsantrags einerseits mit der für einen Datenzugang erforderlichen Spezifikation der von dem Datenzugangsbegehren betroffenen Datensätze und andererseits mit den mit einem Datenzugang verbundenen Risiken für Dritte, insb. für ihr informationelles Selbstbestimmungsrecht. Die Forschungsfreiheit kann und soll den mit einem Datenzugang verbundenen (wenn auch geringen, da es sich zumindest um pseudonymisierte Daten handelt) Eingriff in das informationelle Selbstbestimmungsrecht nur rechtfertigen, wenn tatsächlich ein konkretes Forschungsvorhaben durchgeführt werden soll.

§ 8 Abs. 1 KrebsRegG-E fordert im Antrag eine nachvollziehbare Darlegung, dass der Umfang und die Struktur der beantragten Daten geeignet und erforderlich sind, um die zu untersuchenden Fragen zu beantworten und die Angabe des Vorhabens, das mit den beim Zentrum für Krebsregisterdaten vorliegenden Daten bearbeitet werden kann und eine länderübergreifende Auswertung erfordert. § 8 Abs. 6 fordert eine nachvollziehbare Darlegung, dass die Bereitstellung pseudonymisierter Einzeldatensätze für die Durchführung des Forschungsvorhabens erforderlich ist. Insgesamt haben die Vorgaben der §§ 303e und § 8 KrebsRegG ebenfalls Schutzkonzeptcharakter, wobei die Anforderungen insgesamt geringer sind als im Online-Wirtschaftssektor, was auch damit zu erklären sein dürfte, dass hier die grundrechtlich geschützten Interessen privater Zugangsverpflichteter nicht betroffen sind, sondern allein die Grundrechte der vom Datenzugangsanspruch Drittbetroffenen.

§ 13 BayKrebsRegG setzt die Glaubhaftmachung eines berechtigten, insb. wissenschaftlichen Interesses im Antrag voraus (dazu später: Beweislastverteilung[192]).

cc) Mobilitätssektor

Weder § 63a Abs. 5 StVG noch § 1g Abs. 5 StVG stellen zusätzliche Anforderungen an den Antrag auf Gewährung von Datenzugang. Dies ist auch und gerade damit zu erklären, dass von dem Datenzugangsanspruch weder dem Betriebsgeheimnis unterliegende Daten des Zugangsadressaten

[192] S. dazu: VIII. 9. Beweislastverteilung.

noch personenbezogene Daten Dritter erfasst sind und dass durch einen Datenzugang entstehende Risiko für die Grundrechte anderer Personen daher äußerst gering ist.

4. Schranken

a) Ergebnisse

Für die Anspruchsbegrenzung ergibt sich Folgendes:

1. Der Datenzugang zugunsten von Wissenschaft und Forschung wird de lege lata in der Mehrzahl der Forschungsklauseln nicht unbeschränkt gewährleistet, sondern wird begrenzt. Dies ist Ausdruck eines Ausgleichs der verschiedenen Grundrechtspositionen von Anspruchsberechtigtem, Anspruchsverpflichtetem und Drittbetroffenen.

2. Die Schrankenregelungen der Forschungsklauseln fallen geringer aus, je eingeschränkter der Anwendungsbereich der Forschungsklausel ausgestaltet ist und je weitreichender die Anforderungen an ein bei Antragstellung vorzulegendes Schutzkonzept oder zusätzliche Antragsvoraussetzungen (z.B. Antragstellung durch eine Drittstelle wie dem Koordinator für digitale Dienste) ausfallen. Dies findet seine Begründung darin, dass bereits auf Ebene von Anwendungsbereich, Antragsgestaltung und Schutzkonzept den Grundrechten der Zugangsadressaten und der Dritten weitreichend Rechnung getragen wird, sodass die Schrankenregelungen selbst eingeschränkter ausfallen können.

b) Übersicht

Forschungsklausel	Sektor	Schranken
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	Entgegenstehen überwiegender schutzwürdiger Interessen des Diensteanbieters
§ 5a NetzDG	Online-Wirtschaft	Erhebliches Überwiegen der schutzwürdigen Interessen des Betreibers des sozialen Netzwerkes gegenüber dem öffentlichen Interesse an der Forschung oder Beeinträchtigung der schutzwürdigen Interessen der betroffenen Personen, wenn zugleich das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse der betroffenen Personen nicht überwiegt
Art. 31 DSA-E	Online-Wirtschaft	Plattform ist außerstande, Zugang zu den angeforderten Daten zu gewähren, weil sie keinen Zugriff auf die Daten hat oder die Gewährung des Zugangs zu den Daten zu erheblichen Schwachstellen bei der Sicherheit ihres Dienstes oder beim Schutz vertraulicher Informationen, insb. von Geschäftsgeheimnissen, führt. In diesem Fall

		müssen Vorschläge für ein oder mehrere Alternativen unterbreitet werden, wie der Zugang zu den angeforderten Daten oder zu anderen Daten gewährt werden kann, die für die Zwecke des Verlangens angemessen und ausreichend sind.
§ 303e Abs. 1, Abs. 3 S. 1-3 SGB V	Gesundheit	keine
§ 303e Abs. 3 S. 4 SGB V	Gesundheit	keine
§ 303e Abs. 4 SGB V	Gesundheit	keine
§ 8 Abs. 1 KregregisterG-E § 8 Abs. 6 Krebsregistergesetz-E	Gesundheit	Ausschluss des Antragstellers bei Verstoß gegen Anschlussnutzungsbestimmungen
§ 13 Abs. 1 S. 1 BayKRegG § 13 Abs. 1 S. 2 Bay KrebsRegG	Gesundheit	keine
§ 1g Abs. 5 StVG	Mobilität	keine
§ 63a Abs. 5 StVG	Mobilität	keine

c) Erläuterungen

Schutzwürdige Interessen des Diensteanbieters stehen dem Zugangsrecht nach § 19 Abs. 3 UrhDaG entgegen, wenn sie das öffentliche Interesse an der Forschung überwiegen. Es ist also eine Abwägung der betroffenen Grundrechte vorzunehmen. Ein Überwiegen kann insb. in Betracht kommen, wenn Geheimhaltungsinteressen des Diensteanbieters in unzumutbarer Weise beeinträchtigt würden. Eine bloße Beeinträchtigung reicht nicht aus, sie muss unzumutbar und damit wesentlich ausfallen. Hieraus kann geschlussfolgert werden, dass der Gesetzgeber grundsätzlich von einem Überwiegen des Forschungsdatenzugangsinteresses ausgeht. Nur im Einzelfall kann die Grundrechtsabwägung durch Darlegungen des Diensteanbieters zugunsten seines Geheimhaltungsinteresses ausfallen.

Auch § 5a NetzDG ist begrenzt. Der Datenzugang kann verweigert werden, wenn ein erhebliches Überwiegen der schutzwürdigen Interessen des Betreibers des sozialen Netzwerkes gegenüber dem öffentlichen Interesse an der Forschung festzustellen ist oder die schutzwürdigen Interessen der betroffenen Personen beeinträchtigt werden und das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse der betroffenen Personen überwiegt. Auch hier hebt bereits der Wortlaut der Norm die hohen Voraussetzungen hervor, unter denen der Datenzugang verweigert werden kann. Diese hohen Voraussetzungen rechtfertigen sich auch dadurch, dass der Datenzugangsanspruch auf

sehr spezifische Bereiche beschränkt ist und daher bereits im Anwendungsbereich die Rechte und Interessen von Zugangsadressaten und Dritten hinreichend berücksichtigt wurden. Zusätzlich dient auch das vorzulegende Schutzkonzept dem erforderlichen Grundrechtsausgleich, sodass eine Anspruchsbegrenzung nach Abs. 5 nur noch in spezifischen Einzelfällen in Betracht kommen kann.

Der Anspruch auf Zugang zu Krebsregisterdaten wird für den Zeitraum von bis zu zwei Jahren gänzlich versagt, wenn der Antragsteller gegen die Regelungen der Anschlussnutzung verstößt.

5. Zweckbindung/Regelung der Anschlussnutzung

a) Ergebnisse

Eine Reihe an Forschungsklauseln bindet den Datenzugang an den Zweck der (wissenschaftlichen Forschung), z.T. auch an Gemeinwohlzwecke insgesamt. Eine Zweckbindung des Datenzugangs bedeutet, dass diese Daten zunächst allein für die benannten Zwecke, z.B. zur Durchführung wissenschaftlicher Forschungsvorhaben genutzt werden dürfen. Alternativ oder auch kumulativ finden sich Regelungen der Anschlussnutzung, die sowohl die Ausgangsdaten betreffen können (etwa Anonymisierung nach Abschluss des Forschungsvorhabens oder zweckändernde Anschlussnutzung) als auch die Forschungsergebnisse.

b) Übersicht

Forschungsklausel	Sektor	Zweckbindung des Datenzugangs	Regelung der Anschlussnutzung
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	Zugangsgewährung zum Zweck der wissenschaftlichen Forschung	keine
§ 5a NetzDG	Online-Wirtschaft	keine	Der Forscher darf die Daten ausschließlich verarbeiten für die Zwecke von Vorhaben wissenschaftlicher Forschung nach Abs. 3.
Art. 31 DSA-E	Online-Wirtschaft	Zugangsgewährung zum ausschließlichen Zweck der Durchführung von Forschungsarbeiten, die zur Ermittlung und zum Verständnis systemischer Risiken gemäß Art. 26 Abs. 1 DSA-E beitragen	keine

§ 303e Abs. 1, Abs. 3 S. 1-3 SGB V, § 303e Abs. 3 S. 4 SGB V, § 303e Abs. 4 SGB V	Gesundheit	keine	Soweit die Datenverarbeitung jeweils für die Erfüllung von Aufgaben der nach Abs. 1 Nutzungsberechtigten erforderlich ist, dürfen die Nutzungsberechtigten Daten für folgende Zwecke verarbeiten: 1. Wahrnehmung von Steuerungsaufgaben durch die Kollektivvertragspartner, 2. Verbesserung der Qualität der Versorgung, 3. Planung von Leistungsressourcen, zum Beispiel Krankenhausplanung, 4. Forschung, insb. für Längsschnittanalysen über längere Zeiträume, Analysen von Behandlungsabläufen oder Analysen des Versorgungsgeschehens, 5. Unterstützung politischer Entscheidungsprozesse zur Weiterentwicklung der gesetzlichen Krankenversicherung, 6. Analyse und Entwicklung von sektorenübergreifenden Versorgungsformen sowie von Einzelverträgen der Krankenkassen, 7. Wahrnehmung von Aufgaben der Gesundheitsberichterstattung Die Nutzungsberechtigten dürfen die zugänglich gemachten Daten nach Abs. 5 1. nur für die Zwecke nutzen, für die sie zugänglich gemacht werden, 2. nicht an Dritte weitergeben, es sei denn, das Forschungsdatenzentrum genehmigt auf Antrag eine Weitergabe an einen Dritten im Rahmen eines nach Abs. 2 zulässigen Nutzungszwecks.
§ 8 Abs. 1 KrebsregisterG-E	Gesundheit	Zugangsgewährung zum Zweck der wissenschaftlichen Forschung	Nutzung der Daten nur gestattet für die Zecke, für die sie übermittelt oder bereitgestellt wurden; Weitergabe an Dritte nur gestattet bei Zustimmung des Zentrums für Krebsregisterdaten

§ 8 Abs. 6 KrebsregisterG-E	Gesundheit	Zugangsgewährung zum Zweck der wissenschaftlichen Forschung	Nutzung der Daten nur gestattet für die Zecke, für die sie übermittelt oder bereitgestellt wurden; Weitergabe an Dritte nur gestattet bei Zustimmung des Zentrums für Krebsregisterdaten
§ 13 Abs. 1 S. 1 BayKRegG § 13 Abs. 1 S. 2 BayKRegG	Gesundheit	Berechtigtes, insb. wissenschaftliches Interesse	Frühestmögliche Pseudonymisierung der Daten; Löschung der Daten, sobald sie für die Durchführung oder Überprüfung des Vorhabens nicht mehr erforderlich sind. Werden die Daten länger als fünf Jahre gespeichert, ist die Patientin oder der Patient darauf hinzuweisen
§ 1g Abs. 5 StVG	Mobilität	Übermittlung der Daten nur für verkehrsbezogene Gemeinwohlzwecke, insb. zum Zweck der wissenschaftlichen Forschung im Bereich der Digitalisierung, Automatisierung sowie zum Zweck der Unfallforschung im Straßenverkehr	Verwendung nur für die Übermittlungszwecke
§ 63a Abs. 5 StVG	Mobilität	Übermittlung zum Zwecke der Unfallforschung	keine

c) Erläuterungen

Im Rahmen der Zweckbindung von Forschungsklauseln ist zwischen der Zweckbindung des Datenzugangs und der Zweckbindung der Anschlussnutzung zu differenzieren. § 19 Abs. 3 UrhDaG bindet die Zugangsgewährung allgemein an den Zweck der wissenschaftlichen Forschung. Art. 31 DSA-E konkretisiert dagegen weiter, dass Datenzugang ausschließlich für die Durchführung von Forschungsarbeiten, die zur Erforschung und zum Verständnis „systemischer Risiken“ gemäß Art. 26 Abs. 1 DSA-E beitragen, zu gewähren ist. Regelungen für die Anschlussnutzung finden sich in diesen Klauseln nicht. § 5a NetzDG setzt auf der Ebene der Anschlussnutzung an. Der Forscher darf die Daten hiernach ausschließlich für die Zwecke von Vorhaben wissenschaftlicher Forschung nach Abs. 3 verarbeiten.

6. Weitere Voraussetzungen des Datenzugangs

a) Ergebnisse

Weitere Voraussetzungen des Datenzugangs finden sich in einigen Forschungsklauseln im Kriterium der Erforderlichkeit. § 5a NetzDG fordert beispielsweise, dass die Daten für Vorhaben einer im öffentlichen Interesse liegenden wissenschaftlichen Forschung zu Art, Umfang, Ursachen und Wirkungsweisen öffentlicher Kommunikation in sozialen Netzwerken und den Umgang der Anbieter hiermit erforderlich sein müssen. § 303e Abs. 3 S. 4 SGB V sieht vor, dass Übermittlung aggregierter Daten mit kleinen Fallzahlen erforderlich sein muss, § 303e Abs. 4, dass die Nutzung der pseudonymisierten Einzeldatensätze für einen nach Abs. 2 zulässigen Nutzungszweck, insb. für die Durchführung eines Forschungsvorhabens erforderlich sein muss. Andere Forschungsklauseln sehen einen „besonders begründeten Fall“ als Einschränkung vor, andere die Beteiligung eines wissenschaftlichen Ausschusses bei der Entscheidung über den Datenzugang. All diese zusätzlichen Voraussetzungen haben gemein, dass sie den Datenzugang für Wissenschaft und Forschung einschränken, um dadurch einen Ausgleich mit kollidierenden Grundrechten zu gewährleisten, indem weitere „Safeguards“ zur Wahrung dieser kollidierenden Rechte gewährleistet werden. Diese „Safeguards“ können materiell-rechtlich (durch das Kriterium der Erforderlichkeit) oder formell (durch die Beteiligung von Gremien am Entscheidungsprozess) gewährleistet werden.

b) Übersicht

Forschungsklausel	Sektor	Weitere Voraussetzungen des Datenzugangs
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	keine
§ 5a NetzDG	Online-Wirtschaft	Erforderlichkeit der Daten für Vorhaben einer im öffentlichen Interesse liegenden wissenschaftlichen Forschung zu Art, Umfang, Ursachen und Wirkungsweisen öffentlicher Kommunikation in sozialen Netzwerken und den Umgang der Anbieter hiermit
Art. 31 DSA-E	Online-Wirtschaft	keine
§ 303e Abs. 1, Abs. 3 S. 1-3 SGB V	Gesundheit	keine
§ 303e Abs. 3 S. 4 SGB V	Gesundheit	Erforderlichkeit der Übermittlung aggregierter Daten mit kleinen Fallzahlen
§ 303e Abs. 4 SGB V	Gesundheit	Erforderlichkeit der Nutzung der pseudonymisierten Einzeldatensätze für einen nach Abs. 2 zulässigen Nutzungszweck, insb. für die Durchführung eines Forschungsvorhabens

§ 8 Abs. 1 KrebsregisterG-E § 8 Abs. 6 KrebsregisterG-E	Gesundheit	Beteiligung des wissenschaftlichen Ausschusses
§ 13 Abs. 1 S. 1 BayKRegG	Gesundheit	keine
§ 13 Abs. 1 S. 2 BayKRegG	Gesundheit	Besonders begründeter Fall
§ 1g Abs. 5 StVG	Mobilität	Beachtung von § 26 BDSG
§ 63a Abs. 5 StVG	Mobilität	keine

c) Erläuterungen

Zur Frage, wann eine Erforderlichkeit des Datenzugangs oder der Übermittlung vorliegen soll, schweigen die Forschungsklauseln. Es handelt sich jedenfalls um ein eingrenzendes Kriterium, das auf verschiedene Arten ausgelegt werden kann. Im öffentlich-rechtlichen Kontext ließe es sich einerseits als vorliegend verstehen, sofern kein milderes, gleich geeignetes Mittel existiert, um den mit dem Datenzugang verfolgten Zweck zu erreichen. Andererseits existiert im Rahmen der DSGVO ein Streit über weitere mögliche Lesarten der Erforderlichkeit. Auch bei diesem Streit im Rahmen des Art. 6 Abs. 1 lit. b DSGVO geht es darum, Datenzugang zu personenbezogenen Daten zu erhalten. Die Weitergabe personenbezogener Daten kann danach gerechtfertigt sein, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, *erforderlich* ist. Aus dem Verhältnis von Art. 6 Abs. 1 lit. b DSGVO zu Art. 6 Abs. 1 lit. a DSGVO und Art. 6 Abs. 1 lit. f DSGVO, denen anderenfalls ein großer Teil ihres Anwendungsbereiches genommen würde, ergibt sich, dass Art. 6 Abs. 1 lit. b DSGVO zum Schutze des Betroffenen möglichst eng auszulegen ist. Was erforderlich ist, richtet sich daher nach der vertragscharakteristischen Leistung, die auf ihren eigentlichen Kern reduziert werden muss.[193] Forschungsdatenzugang erfasst dagegen ganz andere Fälle eines Datenzugangs nicht im Privat-, sondern im Gemeininteresse. Das hoch zu gewichtende Interesse daran, Wissenschaft und Forschung im Gemeinwohlinteresse zu gewährleisten, rechtfertigt eine andere Auslegung des Merkmals der Erforderlichkeit. Die Erforderlichkeit sollte daher hier verstanden werden als Notwendigkeit des Datenzugangs für die intendierte Forschung. Die avisierte Forschungstätigkeit darf also ohne die Daten nicht oder nicht auf die gleiche Weise möglich sein. Darauf, ob die Daten auch von einem Dritte oder auf andere Weise erlangt werden können, darf es nach Sinn und Zweck hingegen nicht ankommen.

[193] *Buchner/Petri*, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl., 2020, Art. 6 Rn. 40; *Specht*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl., 2019, § 9 Rn. 48.

7. Vergütungsregelung

Neben den Ergebnissen aus den untersuchten Vorschriften soll – jedenfalls in aller Knappheit – auf Vorgaben aus hier nicht explizit untersuchten Vorschriften hingewiesen sein: Für das Archivrecht beispielsweise ist eine flächendeckende Erhebung von Gebühren vorgesehen und auch das Informationsfreiheitsrecht von Bund und Ländern kennt eine Gebührenpflichtigkeit, ebenso wie das Stasi-Unterlagenrecht. Im Archivrecht existiert aber eine Ausnahme von der Gebührenpflichtigkeit für die wissenschaftliche Nutzung (vgl. z.B. § 4 Abs. 2 BArchKostVO) und im Übrigen ist häufig ein sogenanntes Prohibitionsverbot vorgesehen, nach dem die Gebühren nicht so hoch sein dürfen, dass eine Inanspruchnahme des Informationszugangs verhindert würde (vgl. etwa § 12 Abs. 2 UIG).[194] Insbesondere dieses Prohibitionsverbot scheint geeignet, die Gebührenhöhe angemessen zu begrenzen bei gleichzeitiger Kostendeckung des Zugangsverpflichteten und wird daher im Folgenden aufgegriffen.

a) Ergebnisse

Im Hinblick auf die Vergütungsregeln lassen sich folgende Erkenntnisse festhalten:

1. Im Gesundheitssektor existiert eine umfassende Regelung der Datenzugangsvergütung in der Datentransparenz-Gebührenverordnung (DaTraGebV), die für die Datenzugangsgewährung nach den §§ 303a ff. SGB V gilt. Das bayerische Krebsregistergesetz erlaubt einzig eine vertragliche Kostenregelung.

2. Im Online-Wirtschaftssektor existieren Vergütungsregelungen jedenfalls im nationalen Recht in Form eines Anspruchs auf Erstattung der durch den Datenzugang entstehenden Kosten in angemessener Höhe. Dies ist Ausdruck eines angemessenen Ausgleichs des durch den Datenzugang entstehenden Aufwandes.

3. Vergütungsansprüche sind geeignet, den Datenzugang für Forschung und Wissenschaft unattraktiv auszugestalten und Datenzugang faktisch zu erschweren. § 5a NetzDG sieht daher vor, dass die Kosten kein wesentliches Hindernis für die Inanspruchnahme des Auskunftsrechts darstellen dürfen und normiert damit ebenfalls ein Prohibitionsverbot. Die Kostenhöhe bestimmt sich nach § 287 Abs. 1 ZPO. Außerdem gilt eine Höchstgrenze von 5.000 EUR. Dieser Betrag darf nur überschritten werden, wenn durch die Erteilung der Auskunft ein außergewöhnlich hoher Aufwand entsteht.

[194] Vgl. hierzu ausführlich: *Havel*, Der Informationszugangsanspruch des forschenden Wissenschaftlers, S. 447 ff.

b) Übersicht

Forschungsklausel	Sektor	Vergütung
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	Anspruch auf Erstattung der durch den Datenzugang entstehenden Kosten in angemessener Höhe.
§ 5a NetzDG	Online-Wirtschaft	Anspruch auf Erstattung der durch die Auskunftserteilung nach Abs. 2 entstehenden Kosten in angemessener Höhe. Bei der Bestimmung der angemessenen Höhe ist zu berücksichtigen, dass die Kosten kein wesentliches Hindernis für die Inanspruchnahme des Auskunftsrechts darstellen dürfen. § 287 Abs. 1 ZPO ist entsprechend anzuwenden. Die erstattungsfähigen Kosten dürfen vorbehaltlich des S. 5 höchstens 5.000 EUR betragen. Dieser Betrag darf nur überschritten werden, wenn durch die Erteilung der Auskunft ein außergewöhnlich hoher Aufwand entsteht. Nach Vorlage des Schutzkonzepts nach Abs. 4 kann der Forscher vom Anbieter die Vorlage eines unentgeltlichen Kostenanschlags innerhalb einer angemessenen Frist verlangen.
Art. 31 DSA-E	Online-Wirtschaft	keine
§ 303e Abs. 1, Abs. 3 S. 1-3 SGB V i.V.m. §§ 5 ff. DaTraGebV	Gesundheit	300 EUR Grundgebühr für die Bearbeitung eines Antrages + 300 EUR für die Bereitstellung eines Standarddatensatzes + 300 EUR für die Auswertung und Bereitstellung von Datensätzen + 50-1600 EUR für Beratung, Erstellung vorläufiger Auswertungen und für Zwischenergebnisse abhängig von Umfang und Komplexität der Anfrage und der damit verbundenen Inanspruchnahme von Personal- und Sachleistungen + 100-3000 EUR für Bereitstellung pseudonymisierter Einzeldatensätze in gesicherter physischer oder virtueller Umgebung des Forschungsdatenzentrums
§ 303e Abs. 3 S. 4 SGB V i.V.m. §§ 5 ff. DaTraGebV	Gesundheit	300 EUR Grundgebühr für die Bearbeitung eines Antrages + 300 EUR für die Bereitstellung eines Standarddatensatzes + 300 EUR für die Auswertung und Bereitstellung von Datensätzen + 50-1600 EUR für Beratung, Erstellung vorläufiger Auswertungen und für Zwischenergebnisse abhängig von Umfang und Komplexität der Anfrage und der damit verbundenen Inanspruchnahme von Personal- und Sachleistungen

		+ 100-3000 EUR für Bereitstellung pseudonymisierter Einzeldatensätze in gesicherter physischer oder virtueller Umgebung des Forschungsdatenzentrums
§ 303e Abs. 4 SGB V i.V.m. §§ 5 ff. DaTraGebV	Gesundheit	300 EUR Grundgebühr für die Bearbeitung eines Antrages + 300 EUR für die Bereitstellung eines Standarddatensatzes + 300 EUR für die Auswertung und Bereitstellung von Datensätzen + 50-1600 EUR für Beratung, Erstellung vorläufiger Auswertungen und für Zwischenergebnisse abhängig von Umfang und Komplexität der Anfrage und der damit verbundenen Inanspruchnahme von Personal- und Sachleistungen + 100-3000 EUR für Bereitstellung pseudonymisierter Einzeldatensätze in gesicherter physischer oder virtueller Umgebung des Forschungsdatenzentrums
§ 8 Abs. 1 KrebsregisterG-E § 8 Abs. 6 KrebsregisterG-E	Gesundheit	keine
§ 13 Abs. 1 S. 1 BayKRegG	Gesundheit	Vertraglich zu regeln
§ 13 Abs. 1 S. 2 BayKRegG	Gesundheit	Vertraglich zu regeln
§ 1g Abs. 5 StVG	Mobilität	keine
§ 63a Abs. 5 StVG	Mobilität	keine

c) Erläuterungen

Die Ergebnisse aus der Übersicht sind selbsterklärend und bedürfen keiner weiteren Erläuterung.

8. Frist

a) Ergebnisse

Innerhalb welcher Frist Datenzugang zu gewähren ist, wird durch die untersuchten Forschungsklauseln kaum vorgegeben. Einzig der DSA-Entwurf enthält die Vorgabe, dass der Datenzugang innerhalb einer „angemessenen Frist“ zu gewährleisten ist. Jedenfalls für die öffentlich-rechtlichen Zugangsregelungen, die in der Rechtsfolge eine Ermessensentscheidung vorsehen, kann außerdem auf die allgemeinen Grundsätze zurückgegriffen werden, wonach eine ordnungsgemäße

Ermessensausübung eine Zugangsgewährung in angemessener Zeit erfordert.[195] § 75 S. 2 VWGO sieht hier eine Frist von drei Monaten vor, wenn nicht besondere Umstände eine kürzere Frist gebieten. Datenzugangsbegehren können sehr unterschiedlich im Umfang und auch in der Dringlichkeit ausfallen, weshalb die Normierung genereller Fristen ausscheiden dürfte. Andererseits muss der Forscher aber einen Anhaltspunkt haben, ab welchem Zeitpunkt er ohne das Risiko eines sofortigen Anerkenntnisses mit negativer Kostenfolge für ihn Klage erheben kann. Will man nicht dem Forscher abverlangen, jeweils im Einzelfall Fristen zu setzen, wird man daher um eine gleichermaßen variable wie präzise Fristsetzung nicht herumkommen. In Betracht kommen etwa Formulierungen wie „unverzüglich“ bei gleichzeitiger Setzung einer Höchstfrist. Gleichermaßen ist aber darauf zu achten, dem Datenzugangsadressaten die Möglichkeit der Fristverlängerung in Abhängigkeit von Art und Umfang des Datenzugangsverlangens zu gewähren, um diesen nicht unangemessen zu belasten.

b) Übersicht

Forschungsklausel	Sektor	Frist
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	keine
§ 5a NetzDG	Online-Wirtschaft	keine
Art. 31 DSA-E	Online-Wirtschaft	Angemessene Frist, die von dem Koordinator für digitale Dienste in seinem Verlangen gesetzt wurde. Innerhalb von 15 Tagen nach Eingang eines Verlangens gemäß den Absätzen 1 und 2 kann eine sehr große Online-Plattform den Koordinator für digitale Dienste am Niederlassungsort bzw. die Kommission ersuchen, das Verlangen zu ändern, wenn sie sich aus einem der beiden folgenden Gründe außerstande sieht, Zugang zu den angeforderten Daten zu gewähren [...].
§ 303e Abs. 1, Abs. 3 S. 1-3 SGB V	Gesundheit	keine
§ 303e Abs. 3 S. 4 SGB V	Gesundheit	keine
§ 303e Abs. 4 SGB V	Gesundheit	keine
§ 8 Abs. 1 KrebsregisterG-E § 8 Abs. 6 KrebsregisterG-E	Gesundheit	keine
§ 13 Abs. 1 S. 1 BayKRegG	Gesundheit	keine

[195] *Havert*, Informationszugangsansprüche des forschenden Wissenschaftlers, S. 445 m.w.Nachw.

§ 13 Abs. 1 S. 2 BayKRegG	Gesundheit	keine
§ 1g Abs. 5 StVG	Mobilität	keine
§ 63a Abs. 5 StVG	Mobilität	keine

c) Erläuterungen

Die Ergebnisse sprechen für sich selbst und bedürfen keiner weiteren Erläuterung.

9. Beweislastverteilung

a) Ergebnisse

Hinsichtlich der Beweislastverteilung ist festzustellen, dass diese den allgemeinen Grundsätzen der Darlegungs- und Beweislast folgt, d.h. insb. die Antragsberechtigung durch den Forscher darzulegen ist, häufig auch die Erforderlichkeit der beantragten Daten für das intendierte Forschungsvorhaben.

Der Diensteanbieter hat hingegen die Tatsachen darzulegen und zu beweisen, die einem Forschungsdatenzugang entgegenstehen.

Das Beweismaß wird zugunsten des Forschers z.T. auf eine Glaubhaftmachung abgesenkt, vgl. § 13 BayKRegG.

b) Übersicht

Forschungsklausel	Sektor	Beweislastverteilung
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	Forscher: Berechtigung nach § 60d Abs. 1 und 2 UrhG Diensteanbieter: entgegenstehende überwiegende schutzwürdige Interessen
§ 5a NetzDG	Online-Wirtschaft	Forscher: • Forschereigenschaft • Erforderlichkeit des Datenzugangs für Vorhaben einer im öffentlichen Interesse liegenden wissenschaftlichen Forschung zu Art, Umfang, Ursachen und Wirkungsweisen öffentlicher Kommunikation in sozialen Netzwerken und den Umgang der Anbieter hiermit • Übermittlung des Schutzkonzepts an Diensteanbieter und zuständige Datenschutzaufsichtsbehörde Diensteanbieter: • Verweigerungsgründe nach Abs. 5 • Entstehung der nach Abs. 8 verlangten Kosten durch die Auskunftserteilung

		• Keine Entstehung eines wesentlichen Hindernisses für die Inanspruchnahme des Auskunftsrechts durch die Kostenhöhe • Außergewöhnlich hoher Aufwand durch die Erteilung der Auskunft, der die Überschreitung der Kostenobergrenze von 5.000 EUR rechtfertigt
Art. 31 DSA-E	Online-Wirtschaft	Forscher: • Zulassung nach Abs. 1 und 4 • Beitrag zur Ermittlung und zum Verständnis systemischer Risiken nach Art. 26 Abs. 1 Diensteanbieter: • Außerstandesehen von Zugangsgewährung, weil er entweder keinen Zugriff auf die Daten hat oder weil die Gewährung des Zugangs zu den Daten zu erheblichen Schwachstellen bei der Sicherheit des Dienstes oder beim Schutz vertraulicher Informationen, insb. von Geschäftsgeheimnissen, führen wird
§ 303e Abs. 1, Abs. 3 S. 1 – 3 SGB V	Gesundheit	Forscher: • Anspruchsberechtigung • Eignung und Erforderlichkeit von Umfang und Struktur der beantragten Daten, um die zu untersuchende Frage zu beantworten
§ 303e Abs. 3 S. 4 SGB V	Gesundheit	Forscher: • Anspruchsberechtigung • Zulässiger Nutzungszweck nach Abs. 2 • Erforderlichkeit der Übermittlung der beantragten Daten für den Nutzungszweck nach Abs. 2
§ 303e Abs. 4 SGB V	Gesundheit	Forscher: • Anspruchsberechtigung • Erforderlichkeit der pseudonymisierten Einzeldatensätze für einen nach Abs. 2 zulässigen Forschungszweck • Bereitstellung ausschließlich an Personen, die der Geheimhaltungspflicht nach § 203 StGB unterliegen • Vorhandensein von technischen und organisatorischen Maßnahmen, die sicherstellen, dass die Verarbeitung auf das erforderliche Maß beschränkt ist und ein Kopieren der Daten verhindert werden kann
§ 8 Abs. 1 KrebsregisterG-E	Gesundheit	Forscher: • Eignung und Erforderlichkeit des Umfangs und der Struktur der beantragten Daten,

		um die zu untersuchenden Fragen zu beantworten • Möglichkeit der Bearbeitung des im Antrag angegebenen Vorhabens mit den beim Zentrum für Krebsregisterdaten vorliegenden Daten • Erfordernis einer länderübergreifenden Auswertung
§ 8 Abs. 6 KrebsregisterG-E	Gesundheit	Forscher: • Erforderlichkeit der Bereitstellung pseudonymisierter Einzeldatensätze für die Durchführung des Forschungsvorhabens
§ 13 Abs. 1 S. 1 BayKRegG	Gesundheit	Forscher: • berechtigtes, insb. wissenschaftliches Interesse • Zustimmung des Staatsministeriums bei Übermittlung personenidentifizierender Daten
§ 13 Abs. 1 S. 2 BayKRegG	Gesundheit	Forscher: • berechtigtes, insb. wissenschaftliches Interesse • besonders begründeter Fall, wenn die Übermittlung pseudonymisierter oder personenidentifizierender Daten beantragt wird
§ 1g Abs. 5 StVG	Mobilität	Forscher: • Antragsberechtigung • Übermittlung für verkehrsbezogene Gemeinwohlzwecke
§ 63a Abs. 5 StVG	Mobilität	Forscher: • Antragsberechtigung (Dritte) • Ereignis nach § 7 Abs. 1 StVG • Übermittlung zum Zwecke der Unfallforschung

c) Erläuterungen

aa) Online-Wirtschaftssektor

Die Beweislastverteilung für einen Datenzugangsanspruch gem. § 19a UrhDaG richtet sich mangels abweichender Regelung nach den allgemeinen Grundätzen der Darlegungs- und Beweislast, d.h. jede Partei hat die für sie günstigen Tatsachen darzulegen und zu beweisen. Der Forscher muss also seine Anspruchsberechtigung darlegen und beweisen. Dies beinhaltet seine Tätigkeit, die wissenschaftliche Forschung nach § 60d Abs. 1 und 2 UrhG. Der Einsatz automatisierter oder nicht-automatisierter Verfahren zur Erkennung und Blockierung von Inhalten ist Gegenstand der Auskunftsverpflichtung und nicht Teil der Anspruchsberechtigung und ist daher von der Darlegungs- und Beweislast nicht umfasst.

Entgegenstehende überwiegende schutzwürdige Interessen des Diensteanbieters sind als für diesen günstige Tatsachen vom Diensteanbieter dazulegen und zu beweisen.

Die Beweislast des § 5a NetzDG richtet sich ebenfalls nach den allgemeinen Grundsätzchen. Der Forscher hat danach darzulegen und zu beweisen, dass er als Forscher tätig ist, d.h. wissenschaftliche Forschung betreibt, weiterhin die Erforderlichkeit des begehrten Datenzugangs für Vorhaben einer im öffentlichen Interesse liegenden wissenschaftlichen Forschung zu Art, Umfang, Ursachen und Wirkungsweisen öffentlicher Kommunikation in sozialen Netzwerken und den Umgang der Anbieter hiermit. Auch hat er darzulegen und zu beweisen, dass er ein Schutzkonzept nach § 5a Abs. 4 NetzDG sowohl dem Diensteanbieter als auch der zuständigen Datenschutzbehörde vorgelegt hat.

Der Diensteanbieter hat hingegen die Verweigerungsgründe nach Abs. 5 sowie die Tatsachen im Zusammenhang mit einer geltend gemachten Kostenerstattung nach Abs. 8 darzulegen und zu beweisen. Nach Abs. 5 hat er darzulegen und zu beweisen, dass seine schutzwürdigen Interessen das öffentliche Interesse an der Forschung erheblich überwiegen, oder die schutzwürdigen Interessen der betroffenen Personen beeinträchtigt werden und das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse der betroffenen Personen nicht überwiegt. Das Nichtüberwiegen des öffentlichen Interesses an der Forschung gegenüber dem Geheimhaltungsinteresse der betroffenen Person ist allerdings eine negative Tatsache, die zu einer sekundären Darlegungslast führt, d.h. der Diensteanbieter muss zwar das Geheimhaltungsinteresse der betroffenen Person darlegen, hinsichtlich des Nichtüberwiegens des öffentlichen Interesses an der Forschung kann er sich aber zunächst auf die schlichte Behauptung beschränken. Der Forscher ist dann verpflichtet, dem einfachen Bestreiten mit eigenem qualifizierten Vortrag entgegenzutreten. Dem liegt die Überlegung zugrunde, dass der Forscher die für einen substantiierten Vortrag über das öffentliche Interesse an der Forschung notwendigen Informationen leichter beschaffen kann als der Diensteanbieter. Nach qualifiziertem Vortrag des Forschers aber muss der Diensteanbieter seinen Vortrag konkretisieren und dabei auf das Bestreiten des Forschers eingehen sowie gegebenenfalls Beweis anbieten.

Im Rahmen von Abs. 8 hat der Diensteanbieter die tatsächliche Entstehung der verlangten Kosten durch die Auskunftserteilung dazulegen und ggf. zu beweisen. Außerdem hat er darzulegen und zu beweisen, dass durch die Kostenhöhe kein wesentliches Hindernis für die Inanspruchnahme des Auskunftsrechts entsteht, wobei er sich auch hier nach den Grundsätzen der sekundären Darlegungslast zunächst auf ein bloßes Bestreiten beschränken kann und erst im Falle eines qualifizierten Vortrags des Forschers seinen Vortrag konkretisieren und auf das Bestreiten des Forschers eingehen sowie gegebenenfalls Beweis anbieten muss. Letztlich hat der Diensteanbieter für den Fall, dass die von ihm verlangten Kosten die Obergrenze von 5000,- € überschreiten, darzulegen und gegebenenfalls zu beweisen, dass ihm ein außergewöhnlich hoher Aufwand durch die Erteilung

der Auskunft entstanden ist, der die Überschreitung der Kostenobergrenze von 5000,- € rechtfertigt. Art. 31 DSA-E weist die Besonderheit auf, dass Forscher ihren Zugangsantrag gegenüber dem Koordinator für digitale Dienste am Niederlassungsort der Kommission stellen müssen. Hierin haben sie darzulegen und zu beweisen, dass sie zugelassen sind und dass die Forschungsarbeit, für die Datenzugang begehrt wird, zur Ermittlung und zum Verständnis systemischer Risiken gem. Art. 26 Abs. 1 DSA-E beiträgt. Der Diensteanbieter hingegen muss darlegen und gegebenenfalls beweisen, dass er sich außerstande sieht, Zugang zu den angeforderten Daten zu gewähren, weil er entweder keinen Zugriff auf die Daten hat oder weil die Gewährung des Zugangs zu den Daten zu erheblichen Schwachstellen bei der Sicherheit ihres Dienstes oder beim Schutz vertraulicher Informationen, insb. von Geschäftsgeheimnissen, führen wird.

bb) Gesundheits- und Mobilitätssektor

Die zu beweisenden Tatsachen im Gesundheits- und Mobilitätssektor sind aus der Übersicht erkennbar und bedürfen keiner weiteren Erläuterung. Besonderheiten ergeben sich aber im Beweismaß. § 13 BayKrebsRegG fordert statt der Erbringung des Vollbeweises lediglich eine Glaubhaftmachung.

10. Rechtsdurchsetzung

a) Ergebnisse

Die Rechtsdurchsetzung ist abhängig von der Eröffnung des Rechtsweges. Ob der Zivilrechtsweg oder der Verwaltungsrechtsweg eröffnet ist, beurteilt sich nach allgemeinen Grundsätzen. Besonderheiten ergeben sich allein, wenn Zugangsverpflichteter zwar eine Privatperson ist, Datenzugang aber nur durch eine Dritte Instanz, z.B. den Koordinator für digitale Dienste begehrt werden kann. Bleibt dieser untätig, so ist er auf dem Verwaltungsrechtsweg zum Tätigwerden gegen den privaten Zugangsadressaten zu verpflichten. Der Verwaltungsrechtsweg ist danach immer dann eröffnet, wenn entweder eine aufdrängende Sonderzuweisung diese Rechtsfolge vorsieht oder aber wenn die Voraussetzungen der Generalklausel des § 40 Abs. 1 S. 1 Hs. 1 VwGO erfüllt sind und die Streitigkeit nicht im Wege einer abdrängenden Sonderzuweisung ausdrücklich einer anderen Gerichtsbarkeit zugewiesen wird.

Aufdrängende Sonderzuweisungen liegen für die hier erörterten Forschungsklauseln nicht vor. § 40 Abs. 1 S. 1 HS. 1 VWGO erklärt den Verwaltungsrechtsweg dann für eröffnet, wenn es sich um eine öffentlich-rechtliche Streitigkeit handelt, während die zivilrechtlichen Streitigkeiten von den ordentlichen Gerichten zu entscheiden sind, § 13 GVG. Öffentlich-rechtlich ist eine Streitigkeit, wenn die streitentscheidende Norm öffentlich-rechtlicher Natur ist, d.h. einen Träger öffentlicher Gewalt berechtigt oder verpflichtet. Dies ist im Falle der Forschungsklauseln im Gesundheitssektor de lege lata

sämtlich der Fall. Sind die Forschungsklauseln aber gegen Personen des Privatrechts gerichtet, verpflichten sie allein diese, sodass der Zivilrechtsweg eröffnet ist. Dies ist im Online-Wirtschaftssektor mit § 19 Abs. 3 UrhDaG und § 5a NetzDG der Fall.

Der Verwaltungsrechtsweg ist auch für Streitigkeiten über den nach § 1g Abs. 5 StVG zu gewährenden Datenzugang eröffnet, während der Anspruch aus § 63a Abs. 5 StVG den Halter des Fahrzeugs zum Datenzugang verpflichtet. Hier sind daher die ordentlichen Gerichte zuständig.

b) Übersicht

Forschungsklausel	Sektor	Rechtsdurchsetzung
§ 19 Abs. 3 UrhDaG	Online-Wirtschaft	Zivilrechtsweg: Leistungsklage
§ 5a NetzDG	Online-Wirtschaft	Zivilrechtsweg: Leistungsklage
Art. 31 DSA-E	Online-Wirtschaft	Verwaltungsrechtsweg: Verpflichtungsklage
§ 303e Abs. 1, Abs. 3 S. 1 – 3 SGB V	Gesundheit	Verwaltungsrechtsweg: Verpflichtungsklage
§ 303e Abs. 3 S. 4 SGB V	Gesundheit	Verwaltungsrechtsweg: Verpflichtungsklage
§ 303e Abs. 4 SGB V	Gesundheit	Verwaltungsrechtsweg: Verpflichtungsklage
§ 8 Abs. 1 KrebsregisterG-E	Gesundheit	Verwaltungsrechtsweg: Verpflichtungsklage
§ 8 Abs. 6 KrebsregisterG-E	Gesundheit	Verwaltungsrechtsweg: Verpflichtungsklage
§ 13 Abs. 1 S. 1 BayKRegG	Gesundheit	Verwaltungsrechtsweg: Verpflichtungsklage
§ 13 Abs. 1 S. 2 BayKrebsRegG	Gesundheit	Verwaltungsrechtsweg: Verpflichtungsklage
§ 1g Abs. 5 StVG	Mobilität	Verwaltungsrechtsweg: Verpflichtungsklage
§ 63a Abs. 5 StVG	Mobilität	Zivilrechtsweg: Leistungsklage

c) Erläuterungen

Die Ergebnisse sprechen für sich selbst und bedürfen keiner weiteren Erläuterung.

IX. Internationale Perspektive

In anderen Ländern scheint ein Datenzugang für die Wissenschaft jedenfalls für den Gesundheitssektor bereits zu funktionieren. Positivbeispiele sind hier insb. Finnland, Australien, Kanada, Frankreich und Großbritannien. All diese Rechtsordnungen haben nicht nur Forschungsklauseln, sondern z.T. äußerst ausdifferenzierte Datenzugangsinfrastrukturen entwickelt, in die die Forschungsklauseln eingebunden sind. Es sind daher nicht nur die einzelnen Forschungsklauseln, sondern das Gesamtsystem des Datenzugangs vorzustellen und auf seine Übertragbarkeit zu untersuchen. In den Sektoren Online-Wirtschaft, Mobilität und Energie sind die bereits existenten Forschungsklauseln und Datenzugangsinfrastrukturen weniger vielzählig. Daher wird methodisch der Gesundheitssektor zum Ausgangspunkt der Untersuchung gemacht, die übrigen Sektoren sollten von den Entwicklungen aus dem Gesundheitssektor lernen, ohne dabei freilich die Besonderheiten der betroffenen Sektoren zu vernachlässigen. Die Mehrzahl der gewährten Datenzugangsansprüche für Forschung und Wissenschaft in allen Sektoren richtet sich gegen staatliche Akteure. Wissenschaft und Forschung sollten aber ebenso Zugang zu Datenbeständen Privater bekommen, wobei hier die Grenzen enger zu ziehen sind, um die grundrechtlich geschützten Rechte der Zugangsverpflichteten nicht über Gebühr zu beeinträchtigen. Die Einbindung Privater als Zugangsverpflichtete lässt sich auf verschiedensten Wegen erreichen. Am weitreichendsten scheint hier das indische Modell, weshalb es in den nachfolgenden Ausführungen vorangestellt werden soll (1.), bevor die Forschungsklauseln und Datenzugangsinfrastrukturen für den Gesundheitssektor (2.) und die Sektoren Mobilität (3.) und Energie (4.) erläutert werden.

1. Datenzugang gegenüber staatlichen Stellen und Privaten: Das Beispiel Indien

a) Ergebnisse

In Indien hat das vom Ministry of Electronics and Information Technology (MeitY) eingesetztes Committee of Experts on Non-Personal Data Governance Framework im Dezember 2020 einen Report vorgelegt, der eine Regulierung für nicht-personenbezogene Daten vorschlägt, die u.a. einen (Rechts-)Rahmen für das Teilen nicht-personenbezogener Daten schaffen soll. Ziel ist es v.a. Anreize für Innovation zu geben und den „sozialen, öffentlichen und ökonomischen Wert von Daten zu erschließen“ bei gleichzeitiger Gewährleistung von Privatheitsbelangen.[196]

[196] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 6 (übersetzt durch die Verfasserin), abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.

Nicht personenbezogene Daten im Sinne des Reports sind sämtliche Daten, die von vornherein keinen Personenbezug aufweisen oder ausreichend anonymisiert sind, wobei in Appendix 4 die verwendbaren Anonymisierungstechniken angefügt sind.[197] Zu einer Überschneidung mit dem Datenschutzrecht soll es daher nicht kommen. Mixed Data Sets sollen den Vorgaben des Datenschutzrechts unterliegen.[198]

Dem Problem möglicher De-Anonymisierung soll dadurch entgegengewirkt werden, dass die Daten für den Fall der De-Anonymisierung wieder unter das Datenschutzrecht fallen, sowie durch die Möglichkeit für den Betroffenen, einer Anonymisierung zu widersprechen. Im Falle eines Widerspruchs dürfen die Daten nicht anonymisiert werden und unterliegen von vornherein allein den datenschutzrechtlichen Vorgaben.[199]

Nach dem Report des Expert Committee sollen Rechte an nicht-personenbezogenen Daten begründet werden, die gerade auch das „Recht auf wirtschaftliche und sonstige Wertschöpfung und Maximierung des Nutzens von Daten für die Gemeinschaft“ umfassen. Dieses Recht soll durch verschiedene Gruppen, die typischerweise an der Generierung der Daten beteiligt sind, ausgeübt werden können und gerade nicht nur denjenigen zustehen, die die nicht-personenbezogenen Daten erheben. Damit wird faktisch ein Datenzugangsrecht für jeden an der Generierung und Erhebung der Daten Beteiligten begründet.[200]

b) Übersicht

	Datenzugangsanspruch Data Trust gegenüber Data Custodian	Datenzugangsanspruch Requester gegenüber Data Trust
Anwendungsbereich	• Sektorübergreifender Datenzugangsanspruch • Daten von Unternehmen und Privatpersonen erfasst • Rohdaten und aggregierte Daten erfasst • keine Anwendbarkeit auf „Complete-Datasets“	• Sektorübergreifender Datenzugangsanspruch • High Value Datasets

[197] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 48, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[198] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 10, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[199] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 10 u. 11, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[200] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 11 u. 16, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.

Anspruchsberechtigung	Data Trustee (Regierungsorganisationen und private non-profit Organisationen)	Requester (in Indien registrierte Organisation)
Antragsvoraussetzungen	keine	keine
Regelung der Anschlussnutzung	Nutzung im besten Interesse der von der Datenverarbeitung betroffenen Gruppen	Nutzung im besten Interesse der von der Datenverarbeitung betroffenen Gruppen
Zweckbindung des Datenzugangs	• Sovereign Purpose • Public Good Purpose (u.a. Forschungszwecke) • Nicht: Business Purposes	keine
Schranken	• Geschäftsgeheimnisschutz • Daten, die proprietäre Informationen über Mitarbeiter oder interne Prozess- sowie Produktivitätsdaten umfassen • Gemeinsame Nutzung von Daten verletzt mit einer gewissen Wahrscheinlichkeit die Privatsphäre von Einzelpersonen, Gruppen oder Gemeinschaften	keine
Weitere Voraussetzungen für den Datenzugang	Bei Ablehnung des Datenzugangs durch den Data Custodian positiv beschiedener Antrag beim NPDA	keine
Vergütung	Reasonable charge	Nominal charge
Frist	keine	keine
Beweislastverteilung	Keine Angaben	Keine Angaben
Rechtsdurchsetzung	Rechtsdurchsetzung über die NPDA	Keine Angaben
Einbindung in Datentreuhandstrukturen	ja	ja

Zum Datenzugang verpflichtet ist ein sogenannter Data Custodian, unter dem das Expertenkomitee diejenige Instanz versteht, die die Daten tatsächlich erhebt und speichert. Sie trifft eine Sorgfaltspflicht gegenüber von der Datenverarbeitung betroffenen Gruppen zur ordnungsgemäßen Datenverwaltung. Es kann sich um eine staatliche oder private Entität handeln. Sie soll verpflichtet sein, die Daten für definierte Zwecke mit sogenannten Data Trustees zu teilen, während eine unmittelbare Datenteilungspflicht gegenüber anderen öffentlichen oder privaten Einrichtungen nicht existiert.[201]

[201] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 25, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.

Unter den Begriff des Data Trustees fallen Regierungsorganisationen sowie private non-profit-Organisationen, die sogenannte HVD erstellen, verwalten und teilen. Data Trustees haben dabei u.a. sicherzustellen, dass HVD nur im Interesse des Gemeinwohls verwendet werden.

HVD sind solche Data-Sets, von denen die Allgemeinheit profitieren kann und die daher als öffentliches Gut nach bestimmten Guidelines geteilt werden sollen. Der Data Trustee kann die Erstellung eines HVD bei der Non-Personal Data Authority (NPDA) beantragen, der die Entscheidung über die Erstellung und Verwaltung der HVD obliegt[202] und die von einem Expertenbeirat unterstützt werden soll.[203] Die einschlägigen Guidelines für diesen Prozess sehen insb. vor, dass Daten nur für bestimmte und spezifisch definierte Zwecke geteilt werden müssen, die einem „höheren Allgemeininteresse" dienen.[204] Dazu gehören insb. Forschungszwecke.[205]

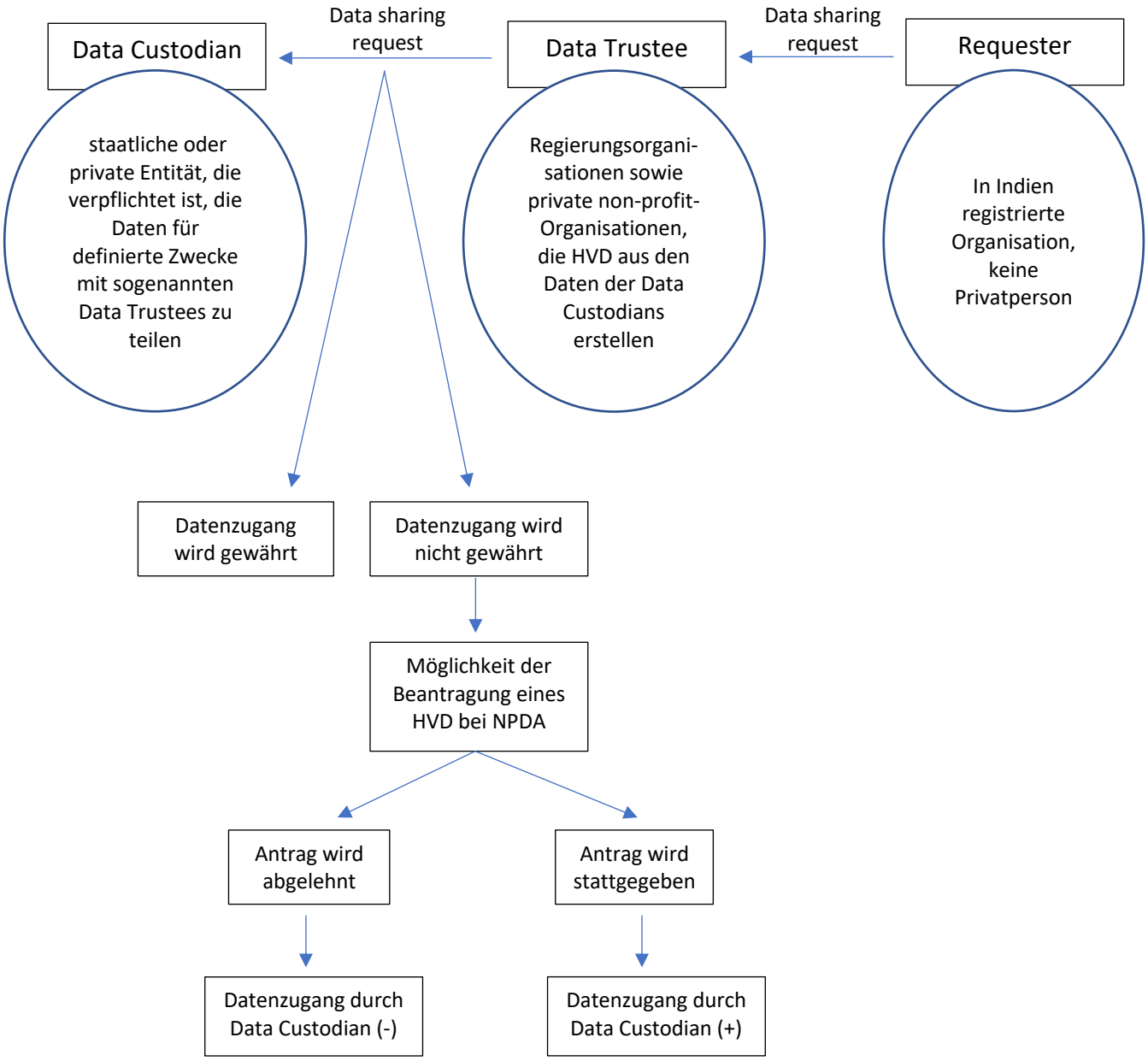
Gegenüber den Data Trustees können wiederum andere „Requester" Datenzugang erhalten, wobei antragsberechtigt nur in Indien registrierte Organisationen sind, keine Privatpersonen.[206] Für die Datenzugangsgewährung kann eine Vergütung („nominal charge") verlangt werden.[207]

Vom Datenzugangsanspruch des Data Trustees gegenüber dem Data Custodian umfasst sind sowohl Rohdaten, als auch aggregierte Daten. Für die Gewährung der Datenteilung von HVD kann eine Vergütung verlangt werden („reasonable charge"), die erforderlichen Zusatzaufwand des Data-Custodians ausgleicht. Dieser Zusatzaufwand liegt beispielsweise in der Anonymisierung der Daten sowie der Gewährleistung des Datenzugangs, nicht aber in der Datenerhebung.[208] Die Datenteilungspflicht unterliegt dann, wenn die Daten privater Unternehmen betroffen sind, den Schranken des Geschäftsgeheimnisschutzes. Nicht von der Datenteilungspflicht erfasst sind außerdem Daten, die proprietäre Informationen über Mitarbeiter oder interne Prozess- sowie

[202] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 19, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[203] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 31, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[204] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 24 (übersetzt durch die Verfasserin), abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[205] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 23, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[206] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 24, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[207] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 30, abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.
[208] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S. 24 (übersetzt durch die Verfasserin), abrufbar unter: https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf, zuletzt abgerufen am 16.07.2021.

Produktivitätsdaten umfassen. Ebenso findet eine Datenteilung nicht statt, wenn die gemeinsame Nutzung von Daten mit einer gewissen Wahrscheinlichkeit die Privatsphäre von Einzelpersonen, Gruppen oder Gemeinschaften verletzt.

Abb. 3: Datenzugangs-Ökosystem Indiens



c) Erläuterung

Der vorgeschlagene Regulierungsrahmen für nicht-personenbezogene Daten in Indien ist hoch innovativ, verfolgt aber ausweislich der im Expertenreport benannten Beispiele v.a. den Zweck, Datenzugang zugunsten des Staates im Gemeinwohlinteresse zu sichern. Datenzugang für

Wissenschaft und Forschung kann und sollte sich nicht allein auf Daten beziehen, die von einer Behörde oder einer Non-Profit Organisation als im öffentlichen Interesse liegende Daten im Sinne eines HVD erklärt werden. Forschung und Wissenschaft benötigt vielmehr Zugang zu nicht vorab definierten Daten. Ob die Forschung selbst dann im öffentlichen Interesse liegen muss, ist eine davon zu unterscheidende Frage. Eine Zwischeninstanz, die den Forschern als Ansprechpartner dient und ihnen den Zugang zu von Dritten erhobenen Daten mittelt, kann den Datenzugangsprozess für die Forscher erleichtern. Nicht zwingend ist es aber, dass die Daten zentral bei dieser Stelle liegen. Vielmehr könnte die Instanz auch den Zugang zu dezentral bei den Unternehmen selbst liegenden Daten mitteln und diese von der zeitlich und ressourcenbelastenden Aufgabe des Datenzugangs entlasten.

Wesentlich für den Forschungsdatenzugang aber ist nicht nur die effektive Zwischenschaltung einer Datenmittelungsinstanz, sondern auch die Tatsache, dass Adressaten des Datenzugangsanspruchs auch private Stellen sein können und dass der Datenzugangsanspruch sektorübergreifend und damit als horizontale Regelung ausgestaltet ist.

2. Internationaler Forschungsdatenzugang im Gesundheitssektor: Die Beispiele Frankreich, Kanada, Finnland, Australien und Großbritannien

a) Frankreich

aa) Ergebnisse

In Frankreich wurde 2018 eine Expertenkommission eingerichtet, die Empfehlungen zur Unterstützung der Nutzung von Gesundheitsdaten erarbeiten sollte.[209] Sie empfahl die Einrichtung eines Datenraumes, der von möglichst vielen Parteien genutzt werden kann und diesen zugänglich ist. Mehrere Projektpartner sollten einen solchen Datenraum erarbeiten, darunter auch Microsoft.[210] „Art. 41 des Loi n. 2019-774 du 24 Juillet 2019 relative à l'organisation et à a transformation du système de santé" ist Rechtsgrundlage dieses Datenraumes. Die konkrete Funktionsausgestaltung wurde im „Arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public «Institut national des données de santé» portant création du groupement d'intérêt public «Plateforme des données de santé" vorgenommen.

Durch diesen Arrêté wird die ehemals als "Institut national des données de santé" bekannte öffentliche Interessenvereinigung in "Plateforme des Données de Santé" umbenannt. In der internationalen Kommunikation wird sie als "Health Data Hub" bezeichnet. Der Health Data Hub hat eine Mitgliederstruktur sowie eine Generalversammlung, die sich aus den Mitgliedern und neun qualifizierten Personen zusammensetzt, darunter der Vorsitzende, die gemeinsam vom Gesundheitsminister und dem Minister für Hochschulbildung, Forschung und Innovation für einen verlängerbaren Zeitraum von fünf Jahren ernannt werden. Die qualifizierten Persönlichkeiten haben eine beratende Stimme. Der Direktor der Plattform und der Vorsitzende der ethischen und wissenschaftlichen Kommission für Forschung, Studien und Evaluationen im Gesundheitsbereich nehmen ebenfalls mit beratender Stimme teil, vgl. Art. 8. Die Plattform wird von einem Board of Directors verwaltet. Die Amtszeit seiner Mitglieder beträgt fünf Jahre und kann verlängert werden. Es setzt sich wie folgt zusammen: zwei Vertreter des Staates und ein Vertreter für die Hochschulen. Den Vorsitz führt der Präsident der Plattform. Dieses Board of Directors entscheidet beispielsweise über die Prüfung von Vorschlägen für vereinfachte Verfahren für den Zugang zu Gesundheitsdaten, Art. 9.1 und 9.4.

---

[209] Arrêté du 5 mai 2017 portant nomination au Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, abrufbar unter: https://www.legifrance.gouv.fr/download/pdf?id=q7JUH89szWx_8vz2eKWIa-yFa-uy6wZupU4KL2icvxY, zuletzt abgerufen am 16.07.2021.

[210] *Cuggia*/*Polton*/*Wainrib*/*Combes*, Health Data Hub: Mission de Préfiguration, 2018, abrufbar unter: https://solidarites-sante.gouv.fr/IMG/pdf/181012_-_rapport_health_data_hub.pdf, zuletzt abgerufen am 16.07.2021.

Im Dezember 2019 wurde eine erste Version des Health Data Hub vorgestellt, im April 2020 wurde sie in den Echtzeitbetrieb genommen. Seit dem 21. April erlaubt ein Ministerialerlass dem Hub, sämtliche Gesundheitsdaten spezifizierter Akteure (s.u.) für die Zwecke der Forschung im öffentlichen Interesse zu erhalten[211] und in der Folge auch bereitzustellen.

bb) Übersicht

	Health Data Hub
Anwendungsbereich	Daten aus den "Gesundheitsdatensystemen"
Anspruchsberechtigung	Wissenschaft und Forschung
Antragsvoraussetzungen	Keine Angabe
Regelung der Anschlussnutzung	Die Nutzung der Daten zu kommerziellen Werbezwecken ist untersagt, die Daten dürfen nicht verkauft werden, die Daten dürfen nicht De-anonymisiert werden
Zweckbindung des Datenzugangs	Wissenschaft und Forschung im öffentlichen Interesse
Schranken	Keine Angabe
Weitere Voraussetzungen für den Datenzugang	Positive Bescheidung durch Ethics Committee
Vergütung	Bislang im Wesentlichen kostenlos; Gegenstand eines Reflektionsprozesses bis 2022
Frist	Keine Angabe
Beweislastverteilung	Keine Angabe
Rechtsdurchsetzung	Keine Angabe
Einbindung in Datentreuhandstrukturen	Health Data Hub ist eine Form der Datentreuhand

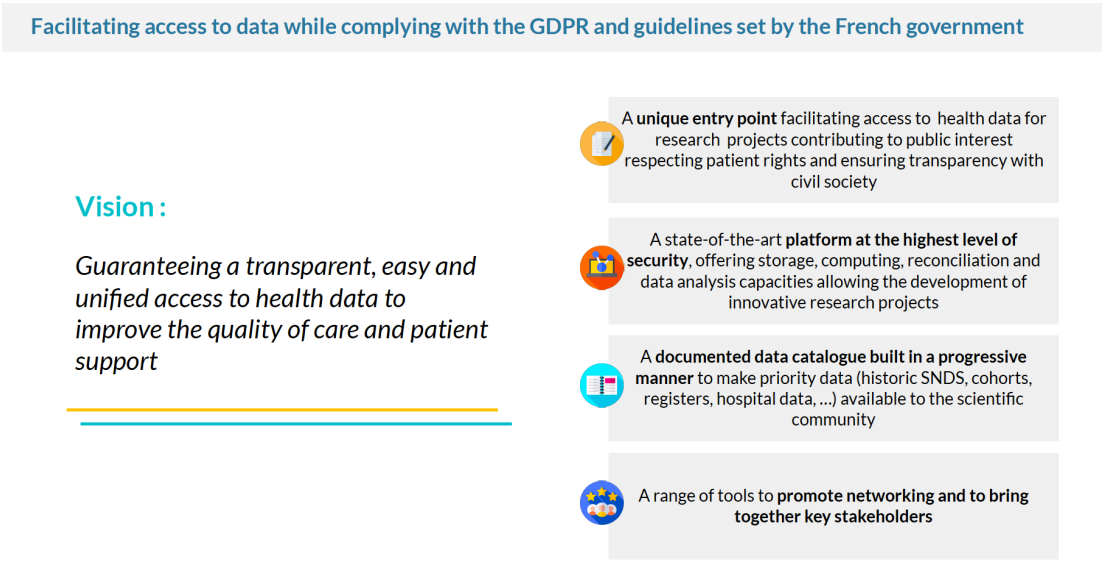
cc) Erläuterungen

In den National Data Hub eingespeist werden Daten des nationalen Gesundheitsdatensystems, vgl. L1462-1 Code de la Santé Publique. Hierzu gehören beispielsweise Krankenversicherungsdaten, Daten von Vorsorgeuntersuchungen, Daten von Mütter- und Kinderschutzdiensten etc. Es handelt sich also um eine Zusammenfassung staatlich erhobener Gesundheitsdaten bei einer Zentralverwaltungsinstanz. Über den Zugang zu den Daten entscheidet ein Ethics Committee, das mit dem Arrêté du 26 mai 2020 portant nomination des membres du Comité éthique et scientifique pour

[211] Arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire, abrufbar unter: https://www.legifrance.gouv.fr/download/file/JQCAhy2BjS_uSuRmKba4o_yPpUVXDsxSS7PEreByYJg=/JOE_TEXTE, zuletzt abgerufen am 16.07.2021.

les recherches, les études et les évaluations dans le domaine de la santé eingerichtet wurde. Es prüft, ob das Forschungsprojekt einen Beitrag zum öffentlichen Interesse leistet. Die Nutzung der Daten zu kommerziellen Werbezwecken ist untersagt, die Daten dürfen nicht verkauft werden.[212] Der Datenzugang zu personenbezogenen Daten im nationalen Gesundheitsdatensystem darf nach L 1461-3 Code de la Santé Publique nur für Zwecke nach L-1461-1 genehmigt werden. Zu diesen Zwecken gehören nach L 1461-1 Abs. 2 Nr. 2 die Zwecke von Forschung, Studien, Evaluationen und Innovation in den Bereichen Gesundheit und medizinisch-soziale Versorgung. Es handelt sich dem Wortlaut des L 1461-1 und L1461-3 um eine echte Forschungsklausel im Sinne eines Datenzugangsanspruchs. Der Zugang zu den in 1461-2 Code de la Santé Publique erfolgt bislang kostenlos. Auch der Zugang zu anderen als den in Artikel L. 1461-2 genannten Gesundheitsdaten ist kostenlos zumindest für Forschung, die ausschließlich für den Bedarf der öffentlichen Verwaltung durchgeführt wird. Die Erarbeitung von Geschäftsmodellen und Finanzierungsmöglichkeiten für den Zugang zu Daten des Health Data Act ist aber Gegenstand eines weiteren Reflektionsprozesses bis 2022.[213] In den Health Data Hub involviert ist auch Microsoft als Infrastruktur-Anbieter, was aber aufgrund der Zugriffsbefugnisse der Geheimdienste auf US-Unternehmen insb. nach dem Schrems II-Urteil des EuGH kritisch gesehen wird.[214] Zusammenfassend wird der Nutzen des Health Data Hub wie folgt dargestellt:

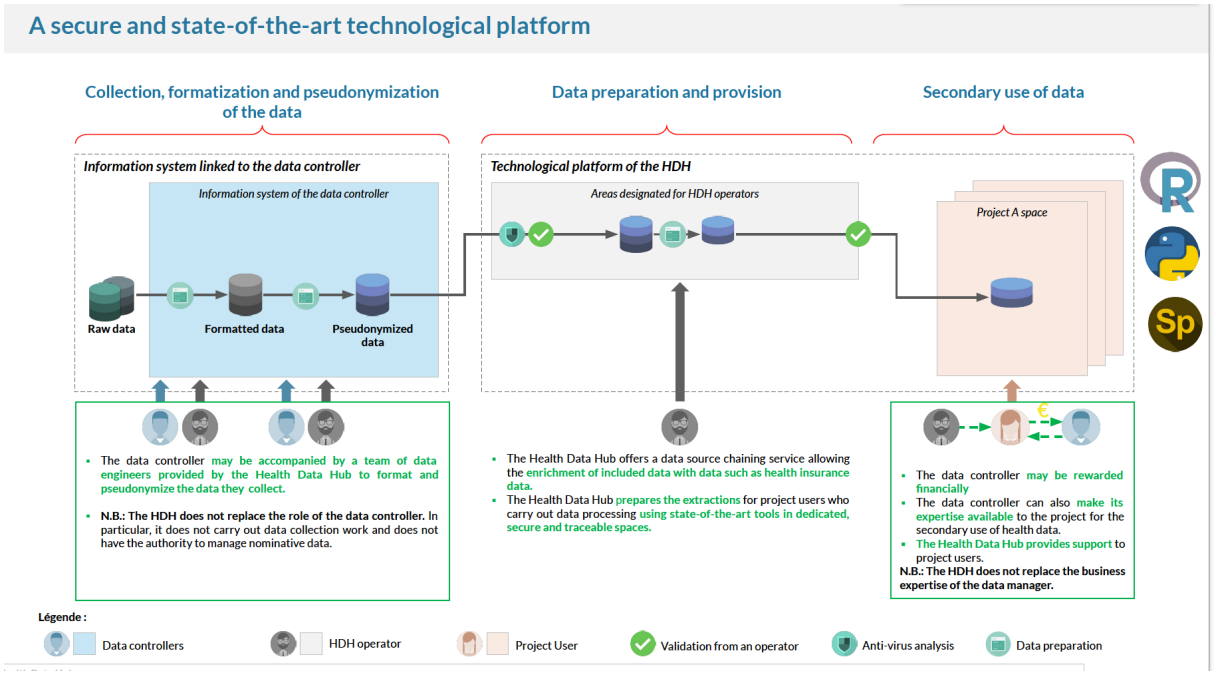
Abb. 4: Stüwe, Präsentation: Health Data Hub - Overview, strategy and lessons learned, 2020[215]



[212] *Stüwe*, Präsentation: Health Data Hub - Overview, strategy and lessons learned, 2020, abrufbar unter: http://ehaction.eu/wp-content/uploads/2020/10/D3S2_HDH-Louisa_Stuwe-new_version.pdf, zuletzt abgerufen am 16.07.2021.
[213] *Stüwe*, Präsentation: G-Colloquium European Public Health Week Forschen mit Gesundheitsdaten - Perspektiven jenseits COVID-19, 2021, S. 14, abrufbar unter: https://goeg.at/sites/goeg.at/files/inline-files/Health%20Data%20Hub(DE)%20-%2020210517.pptx_.pdf, zuletzt abgerufen am 16.07.2021.
[214] Conseil D'État, N° 444937 (Ordonnance du 13 octobre 2020), abrufbar unter: https://www.conseil-etat.fr/content/download/157044/document/444937%20-%20CNLL%20et%20autres.pdf, zuletzt abgerufen am 16.07.2021.
[215] Abrufbar unter: http://ehaction.eu/wp-content/uploads/2020/10/D3S2_HDH-Louisa_Stuwe-new_version.pdf, zuletzt abgerufen am 16.07.2021.

Die einzelnen Prozesse der Datengenerierung und -aufbereitung werden wie folgt dargestellt:

Abb. 5 Stüwe, Präsentation: G-Colloquium European Public Health Week Forschen mit Gesundheitsdaten - Perspektiven jenseits COVID-19, 2021, S. 14[216]



[216] Abrufbar unter: https://goeg.at/sites/goeg.at/files/inline-files/Health%20Data%20Hub(DE)%20-%2020210517.pptx_.pdf, zuletzt abgerufen am 16.07.2021.

b) Kanada

aa) Ergebnisse

In Kanada existieren eine Vielzahl von Regelungen, die es staatlichen Stellen gestatten, Datenzugang für wissenschaftliche Zwecke zu gewährleisten. Diese Datenzugangsansprüche scheinen sich aber sämtlich in der Erlaubnis der Datenzugangsgewährung zu erschöpfen und gerade keinen Anspruch auf Datenzugang zu gewährleisten.[217] Dies ergibt sich aus einer Wortlautanalyse der Vorschriften aus dem Gesundheitsbereich im Vergleich mit Vorschriften aus dem Verwaltungssektor, wo ein Datenzugangsanspruch ausweislich z.B. Art. Chapter IV Devision 2 125 des Act Respecting Access to Documents Held by Public Bodies and the Protection of personal Information[218] durchaus existiert.[219]

Eine Übersicht dieser Erlaubnisse der Datenzugangsgewährung findet sich in einem Papier des "Expert Panels on Timely Access to Health and and Social Data for Health Research and Health System Innovation":[220]

Abb. 6: Accessing health and health-related Data in Canada, The Expert Panel on Timely Access to Health and Social Data for Health Research and Health System Innovation, S. 100-102[221]

Row		Manitoba	Ontario	Quebec
1	De-identified data can be used freely	Yes	Yes	Yes
2	Definition of "identifiable" health information	If the data "allows" identification	Identification is reasonably foreseeable from combination of data	If the data "allows" identification
3	Custodian duties to safeguard data	Must develop information security practices	Must develop information security practices	General duty to take steps to ensure confidentiality
4	Custodian liabilities for data breaches	Investigation by Privacy Commissioner, recommendations by: • Tort liability, including statutory invasion of privacy tort • Possible criminal prosecution	Investigation by Privacy Commissioner, possible orders by: • Tort liability • Possible criminal prosecution	Investigation by Privacy Commissioner, possible orders by: • Tort liability, including statutory invasion of privacy tort • Possible criminal prosecution
5	Data may be used for approved research purposes	Yes	Yes	Yes
6	Approving entity	Designated entity, or other REB that meets statutory test	REB not needing pre- approval but meeting statutory test	Privacy Commissioner
7	Criteria for approval decisions	Lengthy, detailed and/or elaborate legislative standards	Lengthy, detailed and/or elaborate legislative standards	Brief and generally stated
8	Researcher-custodian agreements required	Yes, with extensive and detailed terms	Yes, general duty to get agreements	None required
9	Duties of researchers	Researchers not "trustees," unless a prescribed Health Research Organization	Researchers not "custodians"	Researchers not bound by same duties as custodians
10	Designated research entities	MCHP, CIHI	ICES, CIHI, CCO, POGO	None
11	Disclosures to another province for research	No restrictions	No restrictions	Permitted if receiving jurisdiction has equivalent privacy protections

continued on next page

[217] Office of the Information & Privacy Commissioner for British Columbia, Access to Data for Health Research, 2018, S. 10, abrufbar unter https://www.oipc.bc.ca/guidance-documents/2115, zuletzt abgerufen am 16.07.2021.
[218] Act respecting Acces to Documents held by Public Bodies and the Protection of Personal Information, abrufbar unter http://legisquebec.gouv.qc.ca/en/pdf/cs/A-2.1.pdf, zuletzt abgerufen am 16.07.2021.
[219] Weitere Datenzugangsansprüche für den Verwaltungssektor finden sich im Access to Information Act sowie in Section 5 des Statistic Act i.V.m. Statistics Canada Policy on the Use of Administrative Data Obtained under the Statistics Act.
[220] Accessing health and health-related Data in Canada, The Expert Panel on Timely Access to Health and Social Data for Health Research and Health System Innovation, S. 100-102; abrufbar unter: https://cca-reports.ca/wp-content/uploads/2018/10/healthdatafullreporten.pdf, zuletzt abgerufen am 16.07.2021.
[221] Abrufbar unter: https://cca-reports.ca/wp-content/uploads/2018/10/healthdatafullreporten.pdf, zuletzt abgerufen am 16.07.2021.

Table 4.1

Provincial Legislative Provisions Governing Health Information Privacy and Research Promotion

Row		British Columbia	Alberta	Saskatchewan
1	De-identified data can be used freely	Yes	Yes	Yes
2	Definition of "identifiable" health information	Used but not defined	If identity of person is "readily ascertainable"	Identification is reasonably foreseeable from combination of data
3	Custodian duties to safeguard data	General duty to take steps to ensure confidentiality	Extensive duties to develop and follow information security protocols	Must develop information security practices
4	Custodian liabilities for data breaches	Investigation by Privacy Commissioner, possible orders by: • Tort liability, including statutory invasion of privacy tort • Possible criminal prosecution	Investigation by Privacy Commissioner, possible orders by: • Tort liability • Possible criminal prosecution	Investigation by Privacy Commissioner, recommendations by: • Tort liability, including statutory invasion of privacy tort • Possible criminal prosecution
5	Data may be used for approved research purposes	Yes	Yes	Yes
6	Approving entity	FIPPA: Privacy Commissioner must approve; PIPA: No entity designated	Designated REBs under Regulation	REB approved by Minister
7	Criteria for approval decisions	Brief and generally stated	Lengthy, detailed and/or elaborate legislative standards	Lengthy, detailed and/or elaborate legislative standards
8	Researcher-custodian agreements required	Yes, general duty to get agreements	Yes, with extensive and detailed terms	Yes, with extensive and detailed terms
9	Duties of researchers	Researchers not bound by same duties as custodians	Researchers not "custodians"	Researchers not "trustees", but recipients of health information take on all duties of custodian that disclosed it
10	Designated research entities	None	"health information repository"	None
11	Disclosures to another province for research	Permitted if for approved research	Permitted if custodian enters into agreement with researcher(s) that binds the researchers to protect the confidentiality of the data	No restrictions

continued on next page

Row		New Brunswick	Nova Scotia	Prince Edward Island	Newfoundland & Labrador
1	De-identified data can be used freely	Yes	Yes	Yes	Yes
2	Definition of "identifiable" health information	Identification is reasonably foreseeable from combination of data	Identification is reasonably foreseeable from combination of data	Used but not defined	Identification is reasonably foreseeable from combination of data
3	Custodian duties to safeguard data	Must develop information security practices	Must develop information security practices	General duty to take steps to ensure confidentiality	General duty to take steps to ensure confidentiality
4	Custodian liabilities for data breaches	Investigation by Privacy Commissioner, recommendations by: • Tort liability • Possible criminal prosecution	Investigation by Privacy Commissioner, recommendations by: • Tort liability • Possible criminal prosecution	Investigation by Privacy Commissioner, possible orders by: • Tort liability • Possible criminal prosecution	Investigation by Privacy Commissioner, possible orders by: • Tort liability, including statutory invasion of privacy tort • Possible criminal prosecution
5	Data may be used for approved research purposes	Yes	Yes	Yes	Yes
6	Approving entity	REB not needing pre- approval but meeting statutory test	REB not needing pre- approval but meeting statutory test	Privacy Commissioner	Designated entity or REB approved by provincial HREA
7	Criteria for approval decisions	Lengthy, detailed and/or elaborate legislative standards	Lengthy, detailed and/or elaborate legislative standards	Brief and generally stated	Brief and generally stated
8	Researcher-custodian agreements required	Yes, with extensive and detailed terms	Yes, with extensive and detailed terms	Yes, general duty to get agreements	None required
9	Duties of researchers	"Custodian" includes researchers	Researchers not "custodians"	Researchers not bound by same duties as custodians	Researchers not "custodians"
10	Designated research entities	None	None	None	None
11	Disclosures to another province for research	Permitted if for approved research	Permitted if for approved research	No restrictions	Permitted if for approved research

Auffällig ist, dass die Daten sämtlich „for approved data purposes" genutzt werden dürfen, wobei die Entscheidung über die Nutzung in der Regel von einer hierfür ausgewiesenen Stelle getroffen wird, z.B. von einem „Research Ethics Board" (REB). Außerdem sind Vereinbarungen über die Datennutzung zwischen dem Data Custodian (datenhaltende Stelle) und dem Forscher bzw. der Forschungseinrichtung zu schließen. Im Übrigen sind die Voraussetzungen des Datenzugangs höchst unterschiedlich.

Im Lichte des Papiers des Expert Panels und gewissermaßen als Harmonisierungsmaßnahme der unübersichtlichen Datenzugangslandschaft hat das Ministry of Health in British Columbia eine General Directive für den Zugang zu Gesundheitsdaten für die Forschung erstellt, die allerdings ebenso wie die übrigen Gesetze[222] lediglich normiert, dass das Ministerium unter gewissen Voraussetzungen Zugang zu Daten gewähren kann, hierzu aber nicht verpflichtet ist. Dennoch folgt aus dieser General Directive ein Datenzugangsregime, aus dem zumindest einige Parameter für ein nationales Datenzugangsregime interessant erscheinen und das daher im Folgenden näher erörtert werden soll:

bb) Übersicht

Anwendungsbereich	• Ministry data (personal information) for research purposes • Nicht: Datenzugang aufgrund von Data Sharing Vereinbarungen, z.B. mit der Health Data Coalition
Anspruchsberechtigung	(a) Der Antragsteller muss eine der folgenden Personen sein: (i) eine Person, die eine akademische Position an einer Universität oder Hochschule in Kanada innehat; (ii) ein Doktorand, der an einer Universität oder Hochschule in Kanada eingeschrieben ist und dessen Antrag vom akademischen Betreuer des Doktoranden schriftlich genehmigt wurde; (iii) ein Angehöriger eines Gesundheitsberufs, der bei einer Gesundheitsbehörde in British-Columbia angestellt ist oder dort über Privilegien verfügt; (b) die in dem Antrag beschriebene Forschung muss eine Ethikgenehmigung erhalten haben; (c) die in dem Antrag beschriebene Forschung muss entweder eine schriftliche Genehmigung zur öffentlichen Finanzierung erhalten haben oder anderweitig zur Zufriedenheit des Ministeriums öffentlich finanziert werden oder vom Chief Data Steward zugelassen sein.
Antragsvoraussetzungen	Der Antrag ist in der vom Ministerium vorgesehenen Form zu stellen. Auch der Inhalt kann vom Ministerium vorgegeben werde.
Regelung der Anschlussnutzung	Durch vertragliche Vereinbarung zu regeln
Zweckbindung des Datenzugangs	Forschungszweck
Schranken	Keine Angabe
Weitere Voraussetzungen für den Datenzugang	Im Fall von Daten, aus denen direkte Identifikatoren entfernt wurden, wird das Ministerium die Offenlegung der Daten genehmigen, die vernünftigerweise notwendig sind, um die

[222] Bspw. im British Columbia E-Health (Personal Health Information Access and Protection of Privacy) Act: Part 2 Dev. 3, 14: "The data stewardship committee *may* approve the request".

	vorgeschlagene Forschung durchzuführen, wobei dem öffentlichen Interesse an der Forschung ein erhebliches Gewicht zukommt. Im Fall von persönlichen Daten, die direkte Identifizierungsmerkmale enthalten, wird das Ministerium die Offenlegung nur dann genehmigen, wenn die Forschung vernünftigerweise nicht ohne die Offenlegung von persönlichen Daten durchgeführt werden kann, und wird dann nur die Offenlegung der persönlichen Daten genehmigen, die vernünftigerweise notwendig sind.
Vergütung	Keine Angabe
Frist	Keine Angabe
Beweislastverteilung	Keine Angabe
Rechtsdurchsetzung	Keine Angabe
Einbindung in Datentreuhandstrukturen	nein

cc) Erläuterungen

Erfasst ist Ministry Data mit Personenbezug, wobei ein Datenzugang aufgrund von Data Sharing Vereinbarungen, z.B. mit der Health Data Coalition nicht in den Anwendungsbereich fällt. Die Health Data Coalition (HDC) ist eine von Ärzten geführte Anwendung zur gemeinsamen Nutzung von Daten, die eine Qualitätsverbesserung in der Primärversorgung ermöglichen soll. Die HDC Discover ermöglicht dabei den Zugriff auf einen stets standardisierten und anonymisierten Datensatz, wobei die Vertraulichkeit sowohl für Patienten als auch für Ärzte gewahrt bleibt. Dazu überträgt die HDC Discover Daten aus den verschiedenen elektronischen Krankenakten-Systemen, die von Ärzten in ganz British-Columbia verwendet werden, in eine webbasierte Anwendung.[223]

Die Antragsberechtigung in der General Directive ist auf spezifische Forscher innerhalb Kanadas beschränkt. Besonders hervorzuheben sind zwei Voraussetzungen des Datenzugangs: Erstens, die erforderliche Ethikgenehmigung und zweitens, das zwischen dem Ministerium und dem Forscher abzuschließende Research-Agreement. Es existiert hier eine „Muster-Forschungsvereinbarung" des Ministeriums, die folgende Bestimmungen enthält:

- alle Mitglieder des Forschungsteams müssen eine für das Ministerium zufriedenstellende Datenschutzschulung absolviert haben
- Verbot der Kontaktaufnahme mit Personen, zu deren Daten Zugang gewährt wurde

[223] Für eine Übersicht der Entstehungsgeschichte siehe https://hdcbc.ca/about-us/, zuletzt abgerufen am 16.07.2021.

- jeder Versuch, Personen unter Verwendung der Daten des Ministeriums, allein oder in Kombination mit anderen Informationen, zu identifizieren oder zu re-identifizieren, ist verboten
- Anforderung, individuelle Identifikatoren, falls vorhanden, bei frühestmöglicher Gelegenheit zu beseitigen
- jede nachfolgende Verwendung oder Offenlegung von Daten in individuell identifizierbarer Form ist verboten
- Verpflichtung, angemessene Sicherheitsmaßnahmen zum Schutz der Daten zu implementieren
- die Veröffentlichung jeglicher Informationen, die aus den Daten abgeleitet wurden, oder die Offenlegung der Daten in kleineren als den in der Vereinbarung vorgeschriebenen Zellgrößen ist verboten.

Jeder Verstoß gegen diese vertragliche Verpflichtung begründet eine Haftung des Forschers.

c) Finnland

aa) Ergebnisse

Echte Forschungsklauseln i.S.e. Datenzugangsanspruch zugunsten von Forschung und Wissenschaft kennt das finnische Rechtssystem für den Gesundheitssektor insb. im Biobank-Act 688/2012 sowie im Secondary Use Act. Secondary Use meint – im Gegensatz zum Primary Use – die Nutzung von Daten zu spezifischen anderen Zwecken als diejenigen, für die sie erhoben wurden, vgl. Art. 3 Act on the Secondary Use of Health and Social Data.[224] Ein solcher privilegierter Zweck, für den ein Secondary Use möglich sein soll, ist die Forschung. Art. 38 des Secondary Use Act sieht zwar lediglich vor: *„a data permit may be granted"*. Abs. 2 enthält aber die Vorgabe, dass die Forschungsfreiheit bei der Erteilung der Erlaubnis berücksichtigt werden muss. Dies ließe sich für den Fall, dass einem Datenzugangsanspruch keine Rechte und Interessen des Zugangsverpflichteten oder Dritter entgegenstehen, z.B. Geheimnisschutzerwägungen oder datenschutzrechtliche Gründe, als Begründung eines Anspruchs auf Datenzugang verstehen.

bb) Übersicht

	Act on the Secondary Use of Health and Social Data	Biobank-Act 688/2012
Anwendungsbereich	personenbezogene Daten, die bei der Erbringung von Sozial- und Gesundheitsdienstleistungen erhoben werden, sowie personenbezogene Daten, die zum Zweck der Durchführung, Überwachung, Forschung und Erhebung von Statistiken über den Sozial- und Gesundheitssektor erhoben werden	Generelle Informationen zu den in Biobanken gesammelten Proben (21 Abs. 2)
Anspruchsberechtigung	Personen, die ihre Forschungsfreiheit ausüben	Institution, company, community or individual performing biobank research
Antragsvoraussetzungen	Übermittlung über ein data request management system	keine
Regelung der Anschlussnutzung	Aus den Daten abgeleitete Ergebnisse müssen anonymisiert sein	keine
Zweckbindung des Datenzugangs	Forschung und Wissenschaft	Forschung und Wissenschaft
Schranken		Datenschutz – die bereitgestellten Daten dürfen keinen

[224] *Lilja*, Secondary use of health data – the new Finnish Act, abrufbar unter: https://www.roschier.com/newsroom/secondary-use-of-health-data-the-new-finnish-act/, zuletzt abgerufen am 16.07.2021.

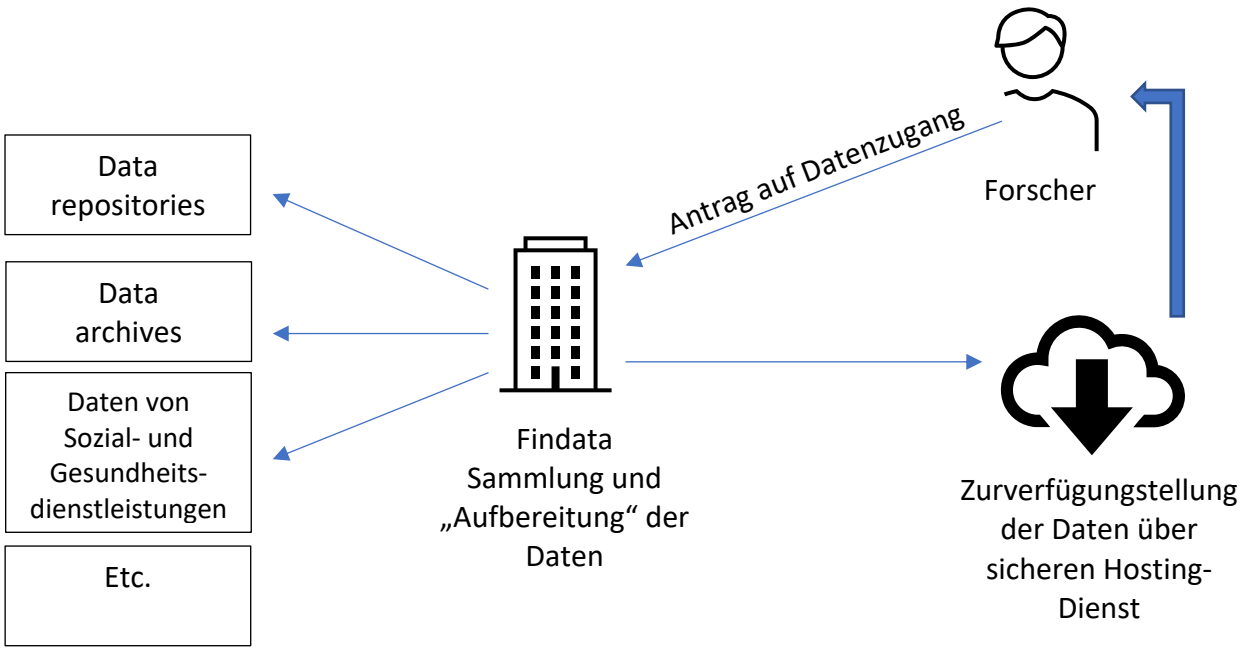
		Personenbezug aufweisen
Weitere Voraussetzungen für den Datenzugang	Nutzung eines sicheren Hosting-Services, ggf. Befristung des Datenzugangs	Informationen müssen für die Beurteilung der Verwendbarkeit der in der Biobank gespeicherten Proben und Informationen erforderlich sein
Vergütung	Erhoben werden kann eine Gebühr für • die Zugangserlaubnis und die Entscheidung über die Zugangsanfrage • Auswahl, Lieferung, Kombination, Vorverarbeitung, Pseudonymisierung und Anonymisierung von Daten sowie für die Nutzung einer sicheren Betriebsumgebung	Keine Angabe
Frist	Die Entscheidung über einen data-permit ist unverzüglich zu treffen, spätestens aber 3 Monate nach Eingang des vollständigen Antrags bei der Behörde, Verlängerung im Einzelfall möglich	Keine Angabe
Beweislastverteilung	Keine Angabe	Keine Angabe
Rechtsdurchsetzung	Keine Angabe	Keine Angabe
Einbindung in Datentreuhandstrukturen	Die Permit-Authority Findata lässt sich als zentrale Datentreuhandinstanz begreifen	nein

cc) Erläuterungen

Erfasst sind Daten sowohl von öffentlichen Stellen, wie national data repositories, healthcare and social welfare care data archives, aber auch registrierte Daten privater Anbieter von Sozial- und Gesundheitsdienstleistungen. Datenzugang wird entweder gewährt durch die datenhaltende Instanz selbst (z.B. das Data Repository) oder durch eine neue Behörde, Findata (Data Permit Authority), die am Finnish Institute for Health and Welfare betrieben wird, von den übrigen Aktivitäten des Institutes allerdings unabhängig ist. Sie untersteht der Aufsicht des Ministry of Social Affairs. Ob Findata oder der Datenhalter selbst für die Erteilung der Erlaubnis zuständig ist, richtet sich nach Sect. 44 des Secondary Use Act. Wird eine Erlaubnis des Datenzugangs durch Findata erteilt, sammelt Findata die Daten von den datenhaltenden Instanzen, kombiniert und pseudonymisiert und anonymisiert sie ggf. (im Folgenden als „Aufbereitung“ der Daten bezeichnet) und stellt sie dem Antragsteller anschließend über einen spezifisch einzurichtenden sicheren Hosting-Service zur Verfügung, vgl. Sect. 10 No. 6

Secondary Use Act. Wird die Erlaubnis von der datenhaltenden Instanz erteilt, werden die Daten ebenfalls über Findata zur Verfügung gestellt, wenn sie vorab pseudonymisiert oder anonymisiert werden müssen. Wurden die Daten auf Grundlage einer datenschutzrechtlichen Einwilligung zur Verfügung gestellt, darf Datenzugang nur gewährt werden, wenn dies von der Reichweite der Einwilligung gedeckt ist, vgl. Sect. 43. Die Daten werden einzig über einen sicheren Hosting-Service bereitgestellt, der von der Permit-Authority betrieben wird, vgl. Sect. 20. Es kann eine Gebühr erhoben werden sowohl für die Zugangserlaubnis und die Entscheidung über die Zugangsanfrage als auch für die Auswahl, Lieferung, Kombination, Vorverarbeitung, Pseudonymisierung und Anonymisierung von Daten sowie für die Nutzung einer sicheren Betriebsumgebung. Die Datenzugangserlaubnis kann befristet oder auch widerrufen werden, vgl. Sect. 43.

Abb. 7: Das Datenzugangsökosystem im Act on Secondary Use of Health and Social Data



Der Biobank Act setzt auf die Möglichkeit einer breiten Einwilligung (broad consent, § 11 Biobank Act) und sieht darüber hinaus ein öffentliches Benachrichtigungsverfahren mit einer Opt-out-Möglichkeit (§ 13) vor. Auch Daten bzw. Metadaten zu den Proben können gem. § 14 Biobank Act gespeichert werden. Diese Daten dürfen durchaus einen Personenbezug aufweisen (§§ 20-23). Der Biobankbetreiber kann den Zugang zu den Sammlungen für Forschungsprojekte im Rahmen des durch das Biobank Act geregelten Umfangs gewähren. Dies umfasst Forschung, die die Biobankproben oder -daten zum Zwecke der Gesundheitsförderung, des Verständnisses von Krankheiten oder der Entwicklung von Produkten und Behandlungsverfahren für die Gesundheit und medizinische Versorgung nutzt. Die Forschung kann wissenschaftliche Interessen oder auch kommerzielle Interessen verfolgen.[225]

Der Zugang zu Biobankproben oder -daten basiert dabei stets auf einer Einzelfallentscheidung für jedes Forschungsprojekt gemäß §§ 26, 27 Biobank Act. Der Antrag muss zu den vorhandenen Proben der Biobank passen und alle gesetzlichen Anforderungen an die Datenverarbeitung erfüllen. Daneben können auch Kriterien, die von der Biobank selbst festgelegt wurden, einzuhalten sein. Auch müssen die Forscher aufzeigen, dass sie beruflich qualifiziert sind, die Daten zu verarbeiten. Zusätzlich sind diese Bedingungen in einem Vertrag zwischen Biobank und dem Empfänger festzuhalten, der stets auch eine Verpflichtung zur Veröffentlichung der Forschungsergebnisse beinhaltet.[226]

Daneben muss der Antragsteller gemäß § 27 einen detaillierten Forschungsplan mit einer ethischen Bewertung und einer Darstellung der geplanten Verarbeitung vorlegen. Die Biobank kann den Zugang ablehnen, wenn der Forschungsbereich nicht zur Biobank passt, die Notwendigkeit besteht, geistige Eigentumsrechte in Bezug auf frühere Forschungen zu sichern, um laufende Forschungsprojekte abzuschließen, um Proben bzw. Daten zu erhalten oder wenn datenschutzrechtliche Gründe oder ethische Gründe dem Datenzugang entgegenstehen.[227]

[225] *Southerington*, Access to Biomedical Research Material and the Right to Data Protection in Finland, in: Slokenberga/Tzortzatou/Reichel, GDPR and Biobanking, Law, Governance and Technology Series, Volume 43, 2021, S. 248.
[226] *Southerington*, Access to Biomedical Research Material and the Right to Data Protection in Finland, in: Slokenberga/Tzortzatou/Reichel, GDPR and Biobanking, Law, Governance and Technology Series, Volume 43, 2021, S. 248.
[227] *Southerington*, Access to Biomedical Research Material and the Right to Data Protection in Finland, in: Slokenberga/Tzortzatou/Reichel, GDPR and Biobanking, Law, Governance and Technology Series, Volume 43, 2021, S. 249.

d) Australien

aa) Ergebnisse

In Australien ist der Zugang zu Forschungsdaten über den My Health Records Act gewährleistet. Das „My Health Record System“ ist ein staatlich betriebenes System zur Bereitstellung von Gesundheitsinformationen über Gesundheitsversorgungsempfänger für die Zwecke der Gesundheitsversorgung des Empfängers (Primärnutzung) sowie für andere Zwecke, z.B. Zwecke von Wissenschaft und Forschung (Sekundärnutzung). Ein Gesundheitsversorgungsempfänger hat eine Gesundheitsakte in diesem System, sobald er sich entweder registriert oder – für den Fall, dass ein Opt-Out-Modell vom Minister angeordnet wird, er nicht ausoptiert. Der Systembetreiber betreibt den National Repositories Service, der die wichtigsten Datensätze der Gesundheitsakte speichert. Andere Datensätze werden von registrierten Repository-Betreibern gespeichert. Zusammen bilden diese Datensätze die Persönliche Gesundheitsakte des Gesundheitsversorgungsempfängers.

bb) Übersicht

Anwendungsbereich	Anonymisierte Daten von Gesundheitsversorgungsempfängern und personenbezogene Gesundheitsdaten
Anspruchsberechtigung	Jedermann mit Ausnahme von Versicherungen
Antragsvoraussetzungen	Beifügung eines Risikomanagement-Plans
Regelung der Anschlussnutzung	Verbotene Zwecke, insb. Nutzung zu spezifischen Versicherungs- und Arbeitgeberzwecken; Monitoring der vereinbarten Anschlussnutzung durch das Board
Zweckbindung des Datenzugangs	Forschungszwecke
Schranken	Privacy-Schutz des Betroffenen
Weitere Voraussetzungen für den Datenzugang	Positive Bescheidung der Datenzugangsbewerbung durch ein Data-Governance Board; Einwilligung des Betroffenen für Zugang zu personenbezogenen Daten; Zustimmung zu den Nutzungsbedingungen
Vergütung	keine
Frist	keine
Beweislastverteilung	Keine Angabe
Rechtsdurchsetzung	Keine Angabe
Einbindung in Datentreuhandstrukturen	Das My Health Record System ist eine Datentreuhand, die Daten sowohl zentral speichert als auch als Datenmittler zwischen externen Drittspeichern und Datennachfragern agiert

cc) Erläuterungen

Wenn ein Empfänger der Gesundheitsfürsorge im System "Meine Gesundheitsakte" registriert ist, kann ein registrierter Gesundheitsdienstleister Gesundheitsinformationen über den Empfänger in das System "Meine Gesundheitsakte" hochladen, es sei denn, der Empfänger der Gesundheitsfürsorge hat den Gesundheitsdienstleister angewiesen, den Datensatz nicht hochzuladen, oder der Datensatz darf aus anderen Gründen nicht hochgeladen werden. Die Registrierung der Gesundheitsdiensteanbieter erfordert einen entsprechenden Antrag sowie die Erfüllung materiell-rechtlicher Voraussetzungen, insb. muss der Gesundheitsdiensteanbieter nach Sec. 9 (1) und Sec. 9A Healthcare Identifiers Act anerkannt werden. Dies setzt voraus, dass der individuelle Gesundheitsdienstleister von einer Registrierungsbehörde als Angehöriger eines Gesundheitsberufs registriert oder Mitglied eines Berufsverbandes ist, der sich auf die Gesundheitsversorgung bezieht, die von dem Mitglied erbracht wurde, wird oder werden soll und einheitliche nationale Mitgliedschaftsanforderungen hat.

Gesundheitsinformationen können aus der persönlichen Gesundheitsakte eines Empfängers der Gesundheitsfürsorge zum Zweck der Forschung vom Systembetreiber zur Verfügung gestellt werden, wenn es sich um anonymisierte Daten handelt oder aber um (personenbezogene) Gesundheitsdaten, sofern der Betroffene zustimmt, Sect. 15 und 83.

Erforderlich ist dafür aber, dass das „Data Governance Board“, das mit verschiedenen Experten besetzt ist und von verschiedenen Gremien beraten wird, einen Antrag auf Nutzung von Daten zu Forschungszwecken positiv bescheidet, Sect. 33 und 109 A. Der Antragsteller muss zuvor den Nutzungsbedingungen zustimmen[228] und einen Risikomanagement-Plan beifügen, auf dessen Grundlage das Board insb. das Risiko eines Verlustes oder Missbrauchs der Daten beurteilt.[229] Für den Zugang zu personenbezogenen Daten ist außerdem stets die Einwilligung des Betroffenen erforderlich. Eine Datenweitergabe an Versicherer findet nicht statt, Sect. 16 und 109 A. Auch spezifische Zwecke der Anschlussnutzung sind untersagt, wobei es sich im Wesentlichen um Zwecke von Versicherungen und Arbeitgebern handelt, Sec. 70 A und 70 B. Die Nutzung von Daten für untersagte Zwecke ist eine Straftat, Sec. 71 A sowie ein Verstoß gegen den Privacy Act 1988, Sec. 72 und 73. Das Board führt ein öffentlich einsehbares Register, aus dem u.a. ersichtlich ist, wer Datenzugang beantragt hat.[230]

---

[228] *Australian Government - Department of Health*, Framework to guide the secondary use of My Health Record system data, S. 31, abrufbar unter: https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf, zuletzt abgerufen am 16.07.2021.

[229] *Australian Government - Department of Health*, Framework to guide the secondary use of My Health Record system data, S. 47, abrufbar unter: https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf, zuletzt abgerufen am 16.07.2021.

[230] *Australian Government - Department of Health*, Framework to guide the secondary use of My Health Record system data, S. 51, abrufbar unter: https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf, zuletzt abgerufen am 16.07.2021.

Spezifische Anforderungen an die Antragsberechtigung bestehen insofern, als jede Entität mit Sitz in Australien den Datenzugang beantragen kann, für Entitäten mit Sitz außerhalb von Australien gelten spezifische Anforderungen.[231] Das Board wendet bei der Bescheidung des Datenzugangsantrags das „Safe-People-Principle“ an und bewertet bei der Zugangsentscheidung ihr Wissen, ihre Fähigkeiten und ihre Anreize, Daten angemessen zu speichern und zu nutzen. Es ist kein Ethikrat. Sofern es feststellt, dass eine ethische Prüfung angezeigt ist, muss es die Zustimmung vom Australian Institute of Health and Welfare (AIHW) einholen.[232] Das „Safe-People Principle“ ist Teil der für den Datenzugang insgesamt entwickelten Security Principles.

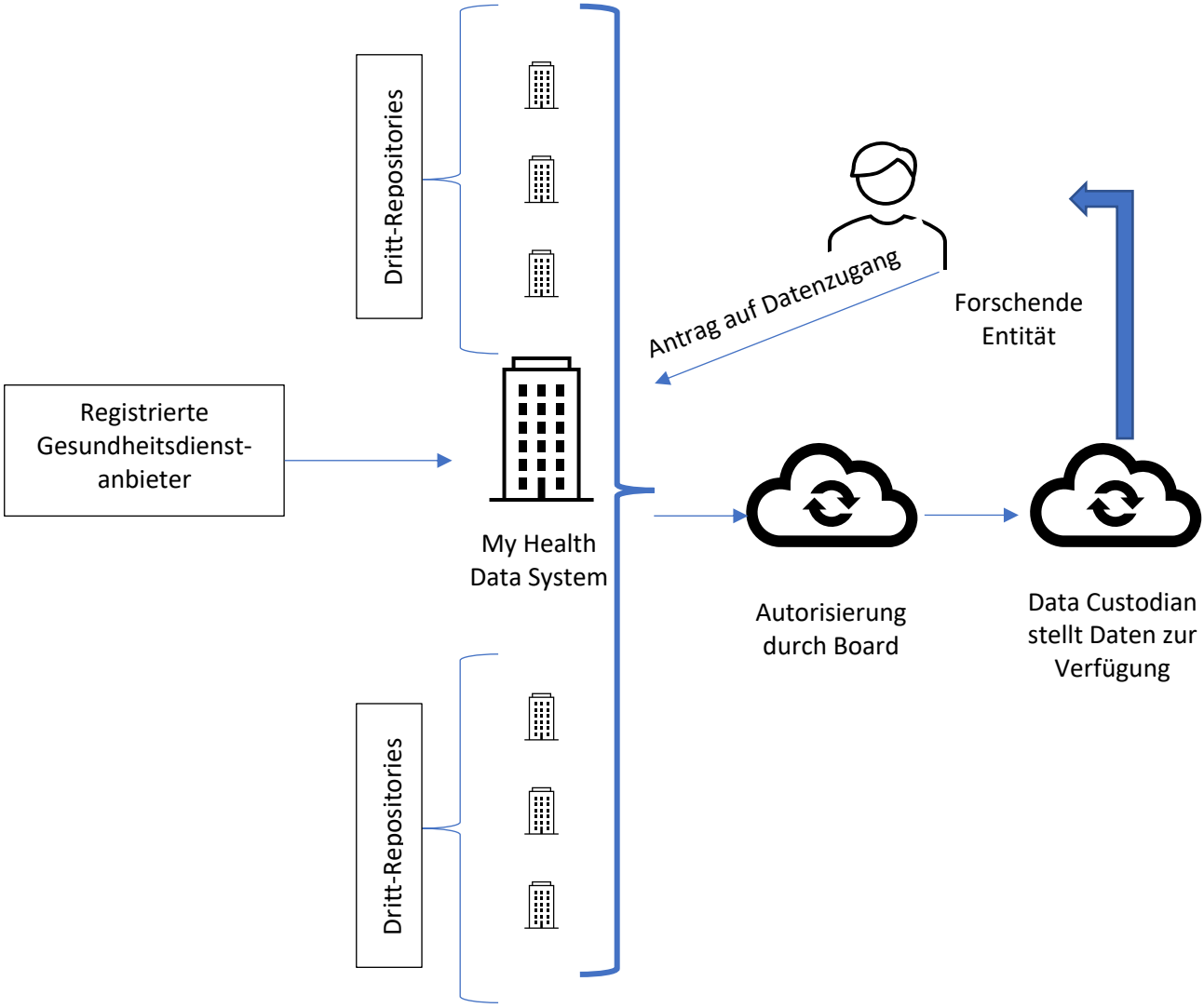
Der Data Custodian – das AIHW – hat nach Sec. 109 A die Aufgabe, Gesundheitsdaten wo erforderlich zu anonymisieren, zu verknüpfen, sie aufzubereiten und Personen bereitzustellen, die zuvor vom Board autorisiert wurden, sowie sicherzustellen, dass die Nutzungsbedingungen eingehalten werden. Der Minister hat die Befugnis, weitere Regeln in Bezug auf die Ausübung dieser Funktionen zu bestimmen.

Das My Health Record System ist eine Datentreuhand, die Daten sowohl zentral speichert als auch als Datenmittler zwischen dezentralen Drittspeichern und Datennachfragern agiert, denn gespeichert werden nicht sämtliche Daten zentral, auch Dritte können sich als Repository bewerben, Sec. 47.

[231] *Australian Government - Department of Health*, Framework to guide the secondary use of My Health Record system data, S. 23, abrufbar unter: https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf, zuletzt abgerufen am 16.07.2021.

[232] *Australian Government - Department of Health*, Framework to guide the secondary use of My Health Record system data, S. 31, abrufbar unter: https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf, zuletzt abgerufen am 16.07.2021.

Abb. 8: Das Datenzugangsökosystem im My Health Records Act



e) Großbritannien

aa) Ergebnisse

In Großbritannien existiert ein System von sieben Research Data Hubs,[233] die im Oktober 2019 von einer unabhängigen, eingetragenen Wohltätigkeitsorganisation, der „Health Data Research UK", eingerichtet wurden. Sämtliche Hubs befinden sich noch in der Aufbauphase, insb. die Frage des Geschäftsmodells ist noch nicht geklärt. Der am weitesten fortgeschrittene Hub ist „Insight". Hier soll Forschung an aggregierten Bilddaten, z.B. Daten aus der Radiologie, ermöglicht werden, indem der Hub als Koordinationsstelle agiert und in dieser Funktion Forschern Zugang zu dezentral bei verschiedenen Gesundheitseinrichtungen, z.B. Krankenhäusern, die als Partner des Hub agieren, gehaltenen Daten mittelt. Die Hubs beruhen auf der britischen Datenstrategie und werden mit öffentlichen Geldern in der Anschubphase gefördert.[234] Es besteht kein Anspruch auf Datenzugang, vielmehr entscheidet ein Gremium nach eigenen festgelegten Kriterien über die Datenzugangsgewährung. Die rechtliche Beurteilung der Datenzugangsgewährung wird durch Anwälte vorgenommen. Werden personenbezogene Daten zur Verfügung gestellt, darf dies allein mit Einwilligung des Betroffenen erfolgen. In dem Data Hub „Insight" hat ein Data Trust Advisory Board (Data TAB) eine Reihe von Zugangskriterien entwickelt, die eine angemessene Prüfung ermöglichen und gleichzeitig praktikabel, effizient und skalierbar sind.[235] Innerhalb des Hubs ist der DataTAB-Vorsitzende Teil des Hub-Führungsteams, der INSIGHT-Direktor nimmt im Gegenzug an allen Sitzungen des DataTAB teil.

bb) Übersicht

	Health Data Hubs
Anwendungsbereich	Gesundheitsdaten
Anspruchsberechtigung	Registrierte Nutzer
Antragsvoraussetzungen	Geschäftsfähigkeit
Regelung der Anschlussnutzung	Nicht geregelt
Zweckbindung des Datenzugangs	Keine Angabe
Schranken	Keine Angabe

[233] Improving UK Health Data: Impacts from Health Data Research Hubs, 2021, abrufbar unter: https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs-v2.pdf, zuletzt abgerufen am 16.07.2021.

[234] *British Government - Department for Digital, Culture, Media & Sport*, National Data Strategy, 2020, abrufbar unter: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy, zuletzt abgerufen am 16.07.2021.

[235] https://theodi.org/article/working-with-the-insight-health-data-research-hub-part-4/, zuletzt abgerufen am 16.07.2021.

Weitere Voraussetzungen für den Datenzugang	Akzeptieren der Nutzungsbedingungen
Vergütung	Kostendeckung; vertraglich bestimmbar
Frist	Keine Angabe
Beweislastverteilung	Keine Angabe
Rechtsdurchsetzung	Keine Angabe
Einbindung in Datentreuhandstrukturen	Der Health Data Research Hub ist eine Datentreuhandstruktur.

cc) Erläuterungen

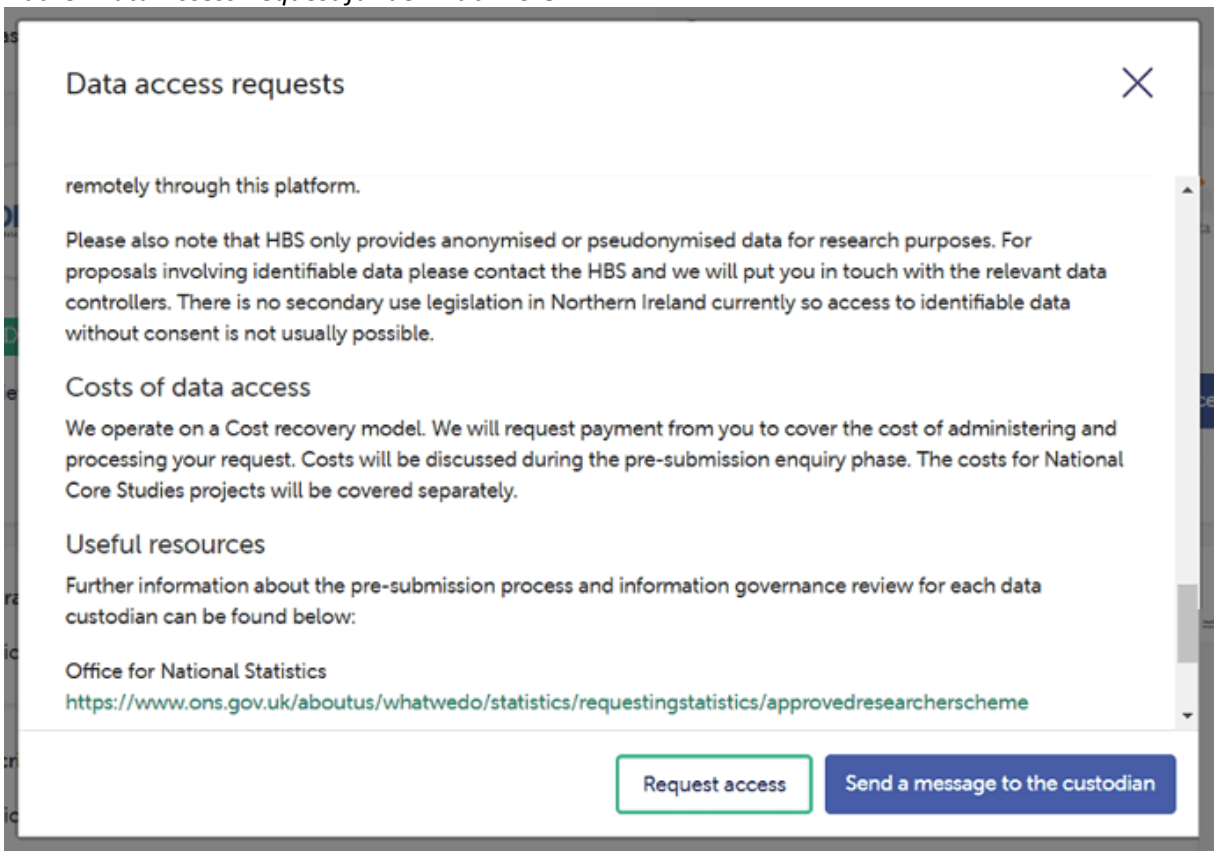
Wird ein Antrag auf Datenzugang in dem Hub INSIGHT gestellt, wird zunächst geprüft, ob dieser rechtskonform und realisierbar ist. Freigegebene Anträge werden an das DataTAB weitergeleitet, um anhand der vom DataTAB entwickelten und am Five Safes Model orientierten Kriterien bewertet zu werden. Das DataTAB gewährt Datenzugang entweder vollumfänglich, mit weiteren Bedingungen oder stellt ihn zurück bis zum Erhalt zusätzlicher Informationen, oder es lehnt den Antrag ab.[236] Die zugangsbetroffenen Daten stammen derzeit von den als Partnern registrierten Krankenhäusern, zukünftig sollen sich aber auch weitere Partner registrieren können. Der Datenzugangsantrag muss über ein standardisiertes Formular gestellt werden und erfordert eine Registrierung. Im Antrag enthalten sein müssen folgende Angaben:[237]

- Name des Antragstellers
- Forschungsziel
- Angaben dazu, ob eine Verknüpfung von Datensätzen erforderlich ist
- Angaben dazu, an welchen Teilen des Datensatzes der Benutzer interessiert ist
- Vorgeschlagenes Datum für den Projektstart
- ICO-Nummer (die Nummer, bei dem der Verantwortliche im Information Commissioner's Office registriert ist)
- Forschungsnutzen (optionales Feld)
- Ethischer Verarbeitungsnachweis (optionales Feld)
- Kontakttelefonnummer (optionales Feld)

[236] Improving UK Health Data: Impacts from Health Data Research Hubs, 2021, abrufbar unter: https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs-v2.pdf, zuletzt abgerufen am 16.07.2021.
[237] https://discourse.healthdatagateway.org/t/introduction-to-data-access-requests/1043, zuletzt abgerufen am 16.07.2021.

Sobald der Benutzer das Anfrageformular ausgefüllt und abgeschickt hat, wird der Inhalt des Formulars per E-Mail an den Datenverantwortlichen zur Prüfung weitergeleitet. Sämtliche Data Hubs können über eine einheitliche Suchfunktion durchsucht werden.

Abb. 9: Data Access Request für den Hub INSIGHT[238]



[238] Abrufbar unter: https://discourse.healthdatagateway.org/t/introduction-to-data-access-requests/1043, zuletzt abgerufen am 16.07.2021.

3. Internationaler Forschungsdatenzugang im Mobilitätssektor: Das Beispiel Australien

a) Ergebnisse

Der Bundesstaat New South Wales (NWS) in Australien arbeitet im Bereich des Forschungsdatenzugangs im Mobilitätssektor mit einem Data Hub (NSW Open Data Transport Hub).[239] Es handelt sich um eine Speicherarchitektur, in der Daten verschiedener Stellen eingespeist und auf vertraglicher Basis freigegeben werden können. Der größte Anteil der Daten kommt vom staatlichen Träger „Transport for New South Wales", z.T. kommen sie aber auch von privaten Dritten. Antragsteller kann nicht allein ein Forscher, sondern jedermann sein. Es werden bspw. Daten zu freiem Parkraum oder der Verfügbarkeit von E-Bikes geteilt.

b) Übersicht

	NSW Open Data Transport Hub
Anwendungsbereich	Im Hub gespeicherte Daten
Anspruchsberechtigung	Registrierte Nutzer
Antragsvoraussetzungen	Geschäftsfähigkeit
Regelung der Anschlussnutzung	Nutzung auf Grundlage der geltenden Gesetze (z.B. der Restriktionen des Immaterialgüterrechts)
Zweckbindung des Datenzugangs	keine
Schranken	keine
Weitere Voraussetzungen für den Datenzugang	Akzeptieren der Nutzungsbedingungen
Vergütung	keine
Frist	keine
Beweislastverteilung	Keine Angabe
Rechtsdurchsetzung	Keine Angabe
Einbindung in Datentreuhandstrukturen	Der Transport Data Hub ist eine Datentreuhandstruktur.

[239] https://opendata.transport.nsw.gov.au, zuletzt abgerufen am 16.07.2021

c) Erläuterungen

Die Angaben aus der Übersicht sprechen für sich selbst und bedürfen keiner weiteren Erläuterung.

4. Internationaler Forschungsdatenzugang im Energiesektor: Das Beispiel Großbritannien

a) Ergebnisse

In Großbritannien wurde im Oktober 2018 vom Department for Business, Energy and Industrial Strategy, dem Amt für Gas- und Strommärkte (Ofgem: Office of the Gas and Electricity Markets) und Innovate UK die Energy Data Taskforce gegründet, um die Regierung, Ofgem und die Industrie zu beraten, wie der Wert von Daten innerhalb des britischen Energiesystems besser genutzt werden kann, um einen stärkeren Wettbewerb zu schaffen, Innovationen bei neuen Produkten, Dienstleistungen und Geschäftsmodellen voranzutreiben und letztendlich ein effizienteres, kostengünstigeres Energiesystem zu schaffen, das im Interesse der Verbraucher funktioniert. Die von dieser Taskforce entwickelten und im Juni 2019 veröffentlichten Empfehlungen[240] enthalten u.a. die Forderung, Daten so weit wie möglich öffentlich zugänglich zu machen und gleichzeitig „kommerziell oder persönlich sensible Daten“ zu schützen.[241]

b) Übersicht

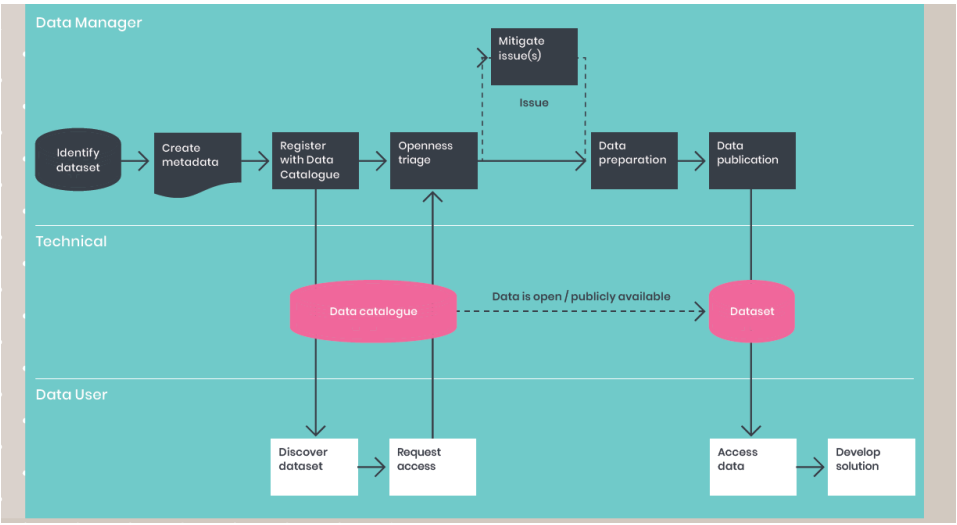
	Energy Data Taskforce
Anwendungsbereich	Energy System Data
Anspruchsberechtigung	Registrierte Nutzer
Antragsvoraussetzungen	Keine Angabe
Regelung der Anschlussnutzung	Vertraglich möglich
Zweckbindung des Datenzugangs	Keine Angabe
Schranken	Keine Angabe
Weitere Voraussetzungen für den Datenzugang	Nutzung des offiziellen Antragsweges im Datenzugangssystem
Vergütung	Keine Angabe
Frist	Keine Angabe
Beweislastverteilung	Keine Angabe
Rechtsdurchsetzung	Keine Angabe
Einbindung in Datentreuhandstrukturen	Keine Angabe

[240] *Sandys* et al., A strategy for a Modern Digitalised Energy System Energy, Data Taskforce report, 2019, abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/Catapult-Energy-Data-Taskforce-Report-A4-v4AW-Digital.pdf, zuletzt abgerufen am 16.07.2021.
[241] https://www.gov.uk/government/groups/modernising-energy-data, zuletzt abgerufen am 16.07.2021.

c) Erläuterungen

Zum Zweck der besseren Zugänglichkeit der Daten sollen Regierung und Ofgem für diesen Zweck den Sektor anweisen, den Grundsatz zu übernehmen, dass die Daten des Energiesystems als offen gelten sollten, wobei die bestehenden gesetzlichen und regulatorischen Maßnahmen entsprechend genutzt werden sollten, unterstützt durch die Anforderungen, dass die Daten "auffindbar, durchsuchbar und verständlich" vorgehalten werden, mit gemeinsamen "Strukturen, Schnittstellen und Standards" und "sicher und widerstandsfähig" sind.[242] Zur Verfügung gestellt werden dynamische, historische und prognostizierende Daten und Statistiken, die das Energiesystem und seinen Betrieb beschreiben.[243] Adressiert wird allerdings lediglich "Energy System Data", die definiert wird als „Fakten und Statistiken, die in einem zugänglichen digitalen Format gesammelt werden und das Energiesystem und seinen Betrieb beschreiben (aktuell, historisch und prognostiziert), einschließlich: Vorhandensein und Zustand der Infrastruktur, Betrieb des Systems, zugehörige Markt Operationen, Politik und Regulierung."[244] Ein „Data Catalogue" soll Metadaten der Datasets zusammenstellen,[245] auf deren Grundlage Datenzugang bei den Datenhaltern beantragt werden kann.[246] Die FAIR Data Principles werden berücksichtigt.

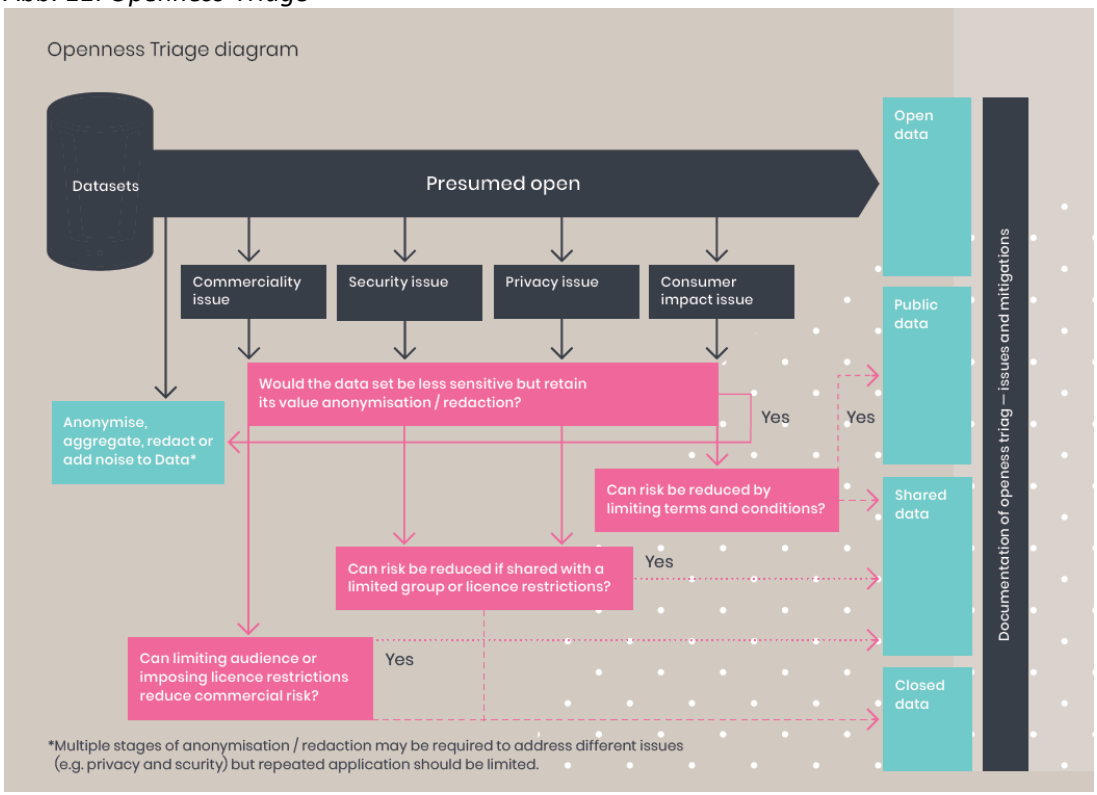
Abb. 10: Datenzugangssystem im Report der Energy Data Taskforce[247]



[242] https://es.catapult.org.uk/reports/energy-data-taskforce-report/, zuletzt abgerufen am 16.07.2021.
[243] Glossary, Energy Data Taskforce Appendix 7, abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/EDTF-Report-Appendix-7-Glossary.pdf, zuletzt abgerufen am 16.07.2021.
[244] *Sandys* et al., A strategy for a Modern Digitalised Energy System Energy, Data Taskforce report, 2019, S. 7, abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/Catapult-Energy-Data-Taskforce-Report-A4-v4AW-Digital.pdf, zuletzt abgerufen am 16.07.2021.
[245] Data Catalogue, Energy Data Taskforce Appendix 2, 2019, abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/EDTF-Report-Appendix-2-Data-Catalogue.pdf, zuletzt abgerufen am 16.07.2021.
[246] Data Catalogue, Energy Data Taskforce Appendix 2, 2019, abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/EDTF-Report-Appendix-2-Data-Catalogue.pdf S. 3 u. 4, zuletzt abgerufen am 16.07.2021.
[247] Abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/Catapult-Energy-Data-Taskforce-Report-A4-v4AW-Digital.pdf, S. 39, zuletzt abgerufen am 16.07.2021.

Diejenigen Stellen, die Daten zur Verfügung stellen, sollen dabei auch und gerade im Rahmen der sog. „Openness Triage“ (siehe nächste Abbildung) festlegen, ob Daten nur anonymisiert oder nur an bestimmte Personengruppen übermittelt werden sollen. Im Rahmen des Entstehungsprozesses des Reports der Energy Data Task Force wurde auch über Ausnahmen von der DSGVO im Gemeininteresse beraten,[248] die letztlich in den Empfehlungen aber nicht aufgegriffen wurden.

Abb. 11: Openness-Triage[249]



Die Tätigkeit der Energy Data Taskforce wird seit dem 12.5.2021 durch eine neue Energy Digitalisation Taskforce (EDiT) fortgesetzt. Ziel ist es auch und gerade, Architekturen und eine Roadmap für die weitere Digitalisierung des Energiesektors zu entwickeln, die auf Erfahrungen aus anderen Branchen zurückgreifen.[250]

Nachdem die „Energy Data Task Force“[251] entsprechende Empfehlungen ausgearbeitet hat, entwickelt zudem Siemens die nationale Energiedatenplattform „YODA“ (Your Online Digital Architecture), über die Energiedaten zugänglich gemacht werden können. Auch zu derartigen Plattformen könnte der Datenzugang für Wissenschaft und Forschung privilegiert gestaltet werden. Siemens arbeitet für das

[248] http://files-eu.clickdimensions.com/techukorg-a6ncz/files/edtf-sprint2techukmeeting.pdf?1553684996289, zuletzt abgerufen am 16.07.2021.
[249] Abrufbar unter: https://esc-non-prod.s3.eu-west-2.amazonaws.com/2019/06/Catapult-Energy-Data-Taskforce-Report-A4-v4AW-Digital.pdf, S. 39, zuletzt abgerufen am 16.07.2021.
[250] https://es.catapult.org.uk/news/energy-digitalisation-taskforce-launches/, zuletzt abgerufen am 16.07.2021.
[251] https://www.gov.uk/government/groups/energy-data-taskforce, zuletzt abgerufen am 16.07.2021.

Projekt „Modernising Energy Data Access“ im Rahmen von Innovate UK (Innovationsagentur der britischen Regierung) zusammen mit den Partnern Energy Systems Catapult (ESC) und dem National Innovation Centre for Data (NICD) an dieser nationalen Energiedatenplattform. YODA will ein besseres lokales Energiemanagement ermöglichen und das Streben nach Dekarbonisierung unterstützen, indem es einen zentralen Energiedatenkatalog, eine Energiekarte der Erzeugung und des Bedarfs sowie ein Anlagenregister für alle neuen Energieanlagen wie Wind- und Solarparks, Ladestationen für Elektrofahrzeuge usw. bereitstellt. Dazu soll die Plattform YODA in sämtliche Daten- und Informationsquellen im gesamten Energiesystem integriert werden.[252]

[252] https://new.siemens.com/uk/en/products/energy/energy-automation-and-smart-grid/modernising-energy-data-access.html, zuletzt abgerufen am 16.07.2021; https://news.siemens.co.uk/news/a-national-energy-data-platform-yoda-have-your-say-on-what-you-need-from-the-platform-to-support-your-business, zuletzt abgerufen am 16.07.2021.

X. Datenzugangsinfrastrukturen

Fehlen Datenzugangsansprüche für Wissenschaft und Forschung, kann eine Datenzugangsgewährung bereits daran scheitern, dass der Aufwand der Datenübermittlung als zu erheblich, riskant oder zu kostenträchtig eingeschätzt, die Haftung für fehlerhafte Datenbestände oder zu Unrecht gewährten Datenzugang gefürchtet wird oder aus anderen Gründen der Wille zur Datenzugangsgewährung schlicht fehlt. Auch dort, wo Datenzugangsansprüche bestehen, ist es aber häufig äußerst mühsam, an die erforderlichen Datenbestände zu gelangen. Dies liegt u.a. daran, dass sie durch die Rechte Dritter, z.B. datenschutzrechtliche und urheberrechtliche Belange und den Geschäftsgeheimnisschutz beschränkt werden und derjenige, der die Daten unter Verstoß gegen die entsprechenden Vorschriften herausgibt, für die Rechtsverletzung haftbar ist. Insb. im Datenschutzrecht besteht dabei eine ganz erhebliche Rechtsunsicherheit, und dies, obwohl die Forschung in der Datenschutzgrundverordnung eine Privilegierung gem. Art. 89 DSGVO erfährt. Erforderlich sind daher Datenzugangsinfrastrukturen, die die Datenzugangsentscheidung treffen und Daten ggf. so aufbereiten, dass ein Datenzugang nicht gegen rechtliche Vorgaben verstößt. Datenzugangsanspruch und Datenzugangsinfrastruktur sollten insofern zwingend zusammengedacht werden. Denn der beste Datenzugangsanspruch hilft nicht, wenn er letztlich aufgrund fehlender institutioneller Einbindung ineffektiv ist.[253] Datentreuhandmodelle könnten Datenzugangsansprüche effektivieren und ein freiwilliges Datenteilen abseits existenter Datenzugangsansprüche befördern. Dies gilt auch für Datenmarktplätze. Die wesentlichen Datenzugangsinfrastruktur-Modelle sollen im Folgenden kursorisch erläutert werden.

a) Forschungsdatenzentren

Es existieren derzeit im Bereich der Sozial-, Verhaltens- und Wirtschaftsswissenschaften 39 Forschungsdatenzentren[254], die vom Rat SWD akkreditiert sind.[255] Diese Forschungsdatenzentren gewähren Datenzugang auf Grundlage eines Nutzungsvertrags, der mit der erforderlichen Anmeldung zustande kommt.[256] Es handelt sich um ein dezentrales System verschiedener

[253] *Specht-Riemenschneider*, Stellungnahme zur öffentlichen Anhörung des Ausschusses Digitale Agenda am 24.2.2021 zur Datenstrategie der Bundesregierung, Berlin 2021, S. 8 ff., abrufbar unter: https://www.bundestag.de/resource/blob/823800/6f11b79c8288a181eaec827c4361825b/Stellungnahme-Specht-Riemenschneider-data.pdf , zuletzt abgerufen am 16.07.2021.

[254] Sämtliche akkreditierte Forschungsdatenzentren finden sich unter: https://www.konsortswd.de/datenzentren/alle-datenzentren/, zuletzt abgerufen am 16.07.2021.

[255] Die Evaluierungskriterien finden sich unter: https://www.konsortswd.de/datenzentren/akkreditierung/, zuletzt abgerufen am 16.07.2021.

[256] Die Nutzungsbedingungen von GESIS und weiteren Forschungsdatenzentren sind hier abrufbar: https://www.gesis.org/fileadmin/upload/dienstleistung/daten/umfragedaten/_bgordnung_bestellen/2018-05-25_Benutzungsordnung_GESIS_DAS.pdf; Forschungsdatenzentrums im BIBB (BIBB-FDZ) teilweise bereitgestellt über GESIS: https://www.bibb.de/dokumente/pdf/Richtlinen_SUF_Nutzung.pdf; Forschungsdaten- und Servicezentrum der Deutschen Bundesbank: https://www.bundesbank.de/resource/blob/604760/bde70332cf1b254bfc34ec3b63d9ffed/mL/gastforscher-information-

Forschungsdatenzentren, die aber zumindest großteilig über eine einheitliche Suchmaschine auf Daten durchsucht werden können. Die Daten der akkreditierten Forschungsdatenzentren können entweder durch externe Stellen eingespeist werden[257] oder aber sie werden durch die Forschungsdatenzentren selbst erhoben, wie dies beispielsweise durch das Sozio-oekonomische Panel geschieht.[258] Forschungsdatenzentren fungieren jedenfalls auch als Datenzugangsmittler. Im Rahmen der nationalen Forschungsdateninfrastruktur sollen diese nationalen Forschungsdatenzentren gestärkt werden, ohne das System als föderale Infrastruktur aber aufzugeben. Die Zugangswege in den FDZ sollen beispielsweise transparenter und einheitlicher gestaltet werden, es soll ein landesweites Netz von Zugangspunkten (z.B. Gastwissenschaftler-Arbeitsplätze in den Forschungsdatenzentren) sowie eine föderierte Archivierungsinfrastruktur aufgebaut werden.[259]

Neben den vom RatSWD akkreditierten Forschungsdatenzentren existieren weitere Registerstellen, wie beispielsweise das Zentrum für Krebsregisterdaten (ZfKD) im Robert Koch-Institut, das die Daten der epidemiologischen Landeskrebsregister auf Bundesebene zusammenführt und sie auf Vollständigkeit und Plausibilität prüft, oder auch das Forschungsdatenzentrum des Bundesinstituts für

data.pdf; LMU-ifo Economics & Business Data Center: https://www.ifo.de/sites/default/files/facts/EBDC/EBDC%20Data%20Archiving%20Agreement_de.pdf; Forschungsdatenzentrum (FDZ) der Bundesagentur für Arbeit (BA) im Institut für Arbeitsmarkt- und Berufsforschung (IAB): http://doku.iab.de/fdz/access/Bearbeitungshinweise_Antrag_SUF.pdf; Leibniz-Institut für Bildungsforschung und Bildungsinformation: https://www.fdz-bildung.de/get_files.php?action=get_file&file=FDZ_Bildung_DV_V3.0.pdf; Forschungsdatenzentrum Betriebs- und Organisationsdaten (FDZ-BO): https://www.diw.de/documents/dokumentenarchiv/17/diw_01.c.672331.de/nutzervertrag_diw_fdz%20bo_muster_deutsch.pdf; Forschungsdatenzentrum des Statistischen Bundesamtes (FDZ-Bund): http://www.forschungsdatenzentrum.de/sites/default/files/fdz_allgemeine_nutzungsbedingungen.pdf; Forschungsdatenzentrum für Hochschul- und Wissenschaftsforschung (FDZ-DZHW): https://www.fdz.dzhw.eu/sites/default/files/data/documente/Datenüberlassungsvertrag_FDZ-DZHW_dt_wiss_Nutzung_2020-04-16_Muster_Website.pdf; Forschungsdatenzentrum am Institut zur Qualitätsentwicklung im Bildungswesen (IQB): https://www.iqb.hu-berlin.de/fdz/Datenuebergabe/Datenbereitstell.pdf; Forschungsdatenzentrum des Leibniz-Instituts für Wirtschaftsforschung Halle (FDZ-IWH): https://www.iwh-halle.de/fileadmin/user_upload/data/benutzerordnung_iwh-fdz_feb-19.pdf; Forschungsdatenzentrum im Kraftfahrt-Bundesamt (FDZ im KBA): https://www.kba.de/DE/Statistik/Forschungsdatenzentrum/Informationen_zur_Datennutzung/muster_pdf.pdf?__blob=publicationFile&v=18; Forschungsdatenzentrum des Leibniz-Instituts für Bildungsverläufe (FDZ-LIfBi): https://www.neps-data.de/Portals/0/NEPS/Datenzentrum/Datenzugangswege/Vertraege/NEPS_Datennutzungsvertrag_de.pdf; Forschungsdatenzentrum PsychData des Leibniz-Institutes für Psychologie (ZPID): https://www.psychdata.de/downloads/pd_nutzung_formular.pdf; Forschungsdatenzentrum Qualiservice: https://www.qualiservice.org/files/contao-theme/public/documents/downloads/Vereinbarung_Datennutzung_01_20202_barrierefrei.pdf; Forschungsdatenzentrum Ruhr am RWI- Leibniz-Institut für Wirtschaftsforschung (FDZ Ruhr am RWI): https://www.rwi-essen.de/forschung-und-beratung/fdz-ruhr/datenzugang/; Forschungsdatenzentrum des Survey of Health, Ageing and Retirement in Europe (SHARE): http://www.share-project.org/data-access/share-conditions-of-use.html; Forschungsdatenzentrum Wissenschaftsstatistik: https://www.fdz-wissenschaftsstatistik.de/download/file/fid/136; Forschungsdatenzentrum des Leibniz-Institut für Finanzmarktforschung SAFE: https://datacenter.safefrankfurt.de/datacenter/documents/Terms_of_Use_Datacenter_01-04-2021.pdf, alle zuletzt abgerufen am 16.07.2021.

[257] So wurden beispielsweise die Befragungsergebnisse des SVRV zum Lagegutachten bei GESIS eingespeist: https://dbk.gesis.org/dbksearch/GDESC2.asp?no=0207&DB=D, zuletzt abgerufen am 16.07.2021.

[258] https://www.diw.de/de/diw_01.c.412809.de/presse/glossar/sozio_oekonomisches_panel_soep.html, zuletzt abgerufen am 16.07.2021.

[259] https://www.konsortswd.de/konsortswd/tasks/datenzugang/, zuletzt abgerufen am 16.07.2021.

Arzneimittel und Medizinprodukte, das Zugang zu von Drittstellen eingespeisten Daten auf Grundlage von § 303e SGB V gewährleistet und daher ebenfalls als Datenmittler auftritt.

b) Data Hubs

Data Hubs finden sich als Datenspeicherarchitektur vermehrt im Ausland, z.B. in Großbritannien und Frankreich sowie in Australien in ganz verschiedenen Sektoren. Ein Data Hub kann als Hub-and-Spoke-Ansatz zum Speichern und Verwalten von Daten betrachtet werden. Dabei werden die Daten von Drittstellen physisch verschoben und in ein neues System exportiert. Die neue Systemumgebung verleiht den Daten mehr Struktur, ein einheitliches Format und ermöglicht es beispielsweise, Daten in Gruppen/Clustern anzuordnen, womit letztlich ein schnellerer Zugriff auf die benötigten Daten sichergestellt wird. Ziele sind v.a. die Reduzierung von Datensilos, Clusterbildung von Daten durch Re-Indizierung in eine neue Systemumgebung, Herstellung von Interoperabilität zwischen den ursprünglichen Datensets aus heterogenen Quellen sowie ein schnelles Auffinden von Daten.[260]

Bisherige Anwendungsfelder sind v.a. gemeinsame Projekte von kooperierenden Unternehmen: Bspw. können sich ein Telekommunikationsbetreiber, eine Bank und ein Supermarkt zusammenschließen, um Erkenntnisse und Datenelemente auszutauschen. Jedes dieser Unternehmen hat Zugang zu grundsätzlich allen gesammelten Daten, die in einem zentralen Repository gehostet werden.[261]

Ein Data Hub unterscheidet sich von einem Data Lake dadurch, dass er Daten homogenisiert bereitstellt und dass er den Daten weiteren Wert hinzufügt, wie beispielsweise eine Deduplizierung, Datenqualitätsanforderungen, Datensicherheit und einen standardisierten Satz von Abfragen ermöglicht. Ein Data Lake speichert Daten grundsätzlich unverändert an einem Speicherort, um sie verfügbar zu machen, und erlaubt/verlangt, dass der Nutzer die Daten selbstständig verarbeitet oder ihnen einen Mehrwert hinzufügt.[262]

c) Datentreuhand

Vermehrt wird spätestens seit ihrer Erwähnung in der Datenstrategie der EU sowie in der nationalen Datenstrategie über Datentreuhandstrukturen nachgedacht. Basierend auf umfassenden Vorarbeiten

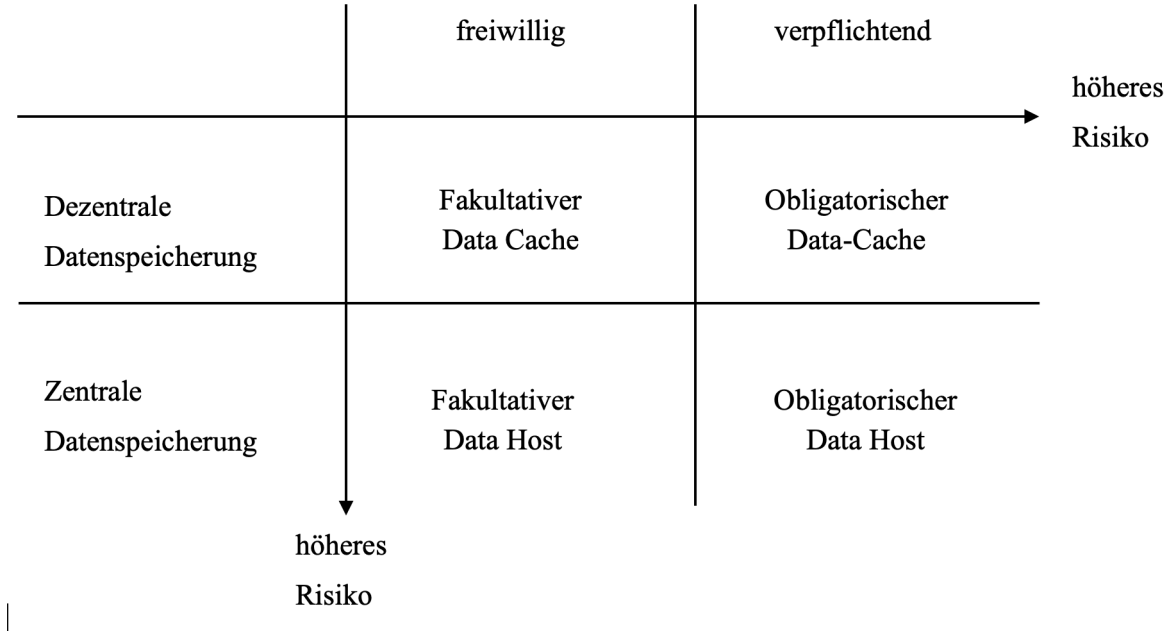
[260] https://www.datacenter-insider.de/was-ist-ein-hub-a-800872/, zuletzt abgerufen am 16.07.2021.
[261] https://www.computerweekly.com/de/tipp/Data-Hub-versus-Data-Lake-Wie-unterscheiden-sie-sich, zuletzt abgerufen am 16.07.2021.
[262] https://www.computerweekly.com/de/tipp/Data-Hub-versus-Data-Lake-Wie-unterscheiden-sie-sich, zuletzt abgerufen am 16.07.2021; https://de.wikipedia.org/wiki/Data_Lake, zuletzt abgerufen am 16.07.2021.
[262] https://www.computerweekly.com/de/tipp/Data-Hub-versus-Data-Lake-Wie-unterscheiden-sie-sich#:~:text=Ein%20Data%20Hub%20kann%20als,einem%20neuen%20System%20re%2Dindiziert., zuletzt abgerufen am 16.07.2021.; https://www.speicherguide.de/datacenter/gegen-das-datenchaos-vom-data-lake-zum-data-hub-24193.aspx, zuletzt abgerufen am 16.07.2021.

zur Datentreuhand, die nachfolgend zusammengefasst wiedergegeben werden[263] soll der Begriff der Datentreuhand hier verstanden werden als

> *„eine natürliche oder juristische Person oder eine Personengesellschaft, die den Zugang zu von Datentreugebern bereitgestellten oder bereitgehaltenen Daten nach vertraglich vereinbarten oder gesetzlich vorgegebenen Daten-Governance-Regelungen (auch) im Fremdinteresse mittelt."*[264]

Weitere Funktionen der Datentreuhand, z.B. die Pseudonymisierung und/oder Anonymisierung oder auch die Datenauswertung können selbstredend hinzukommen. Es existieren vier Grundformen der Datentreuhand, die sich anhand von Zentralität und Dezentralität der Datenspeicherung sowie ihrem fakultativen oder verpflichtenden Einsatz unterscheiden:

Abb. 12: Datentreuhand Matrix[265]



Die hier entwickelte Grundmodellierung entscheidet zwischen freiwilligen (fakultativen) und verpflichtenden (obligatorischen) Datentreuhandmodellen sowie zwischen zentraler und dezentraler Datenspeicherung. Der Einsatz fakultativer Datentreuhandmodelle beruht auf der freien Willensentscheidung der Beteiligten, insb. des Betroffenen oder des technisch-faktischen Dateninhabers. Die Parteien schließen in diesem Zuge einen Datentreuhandvertrag, der Grundlage dieses Rechtsverhältnisses wird. Freiwillige Modelle sind z.B. denkbar für die in der Datenstrategie der Bundesregierung angedachte staatliche Agrardatenplattform, bei Biodatenbanken, für das Teilen von

[263] Die nachfolgenden Ausführungen zur Datentreuhand beruhen auf den Ausführungen aus *Specht-Riemenschneider/Blankertz* et al., Die Datentreuhand, MMR-Beilage 2021, 25, 25-48.
[264] *Specht-Riemenschneider/Blankertz* et al., Die Datentreuhand, MMR-Beilage 2021, 25, 27.
[265] Ebenfalls aus: *Specht-Riemenschneider/Blankertz* et al., Die Datentreuhand, MMR-Beilage 2021, 25, 27.

Krankenhausdaten zu Forschungszwecken oder auch zur Schaffung eines „Circular Data Space“ für digitale Produktpässe.

Der fakultative Data-Cache ist eine freiwillig eingesetzte Datendurchleitungsinstanz, die z.B. die Datenzugangsentscheidung nach gesetzlich oder privatautonom vorgegebenen Zugangsbedingungen trifft. Vorstellbar ist es beispielsweise, dass Kliniken Daten lokal vorhalten und diese für eine Treuhand freigegeben werden, um temporär das Trainieren von Algorithmen zu ermöglichen.

Fakultative Data-Host Modelle beschreiben freiwillig geschaffene Datenräume, bei denen Datenzugang auf Grundlage vertraglich vordefinierter oder gesetzlich vorgegebener Bedingungen vom Datentreuhänder gewährt wird. Die Speicherung erfolgt beim fakultativen Data-Host. Dass die Bedingungen der Datenzugangsgewährung gesetzlich vorgegeben werden oder spezifische rechtliche Anforderungen an die die Zugangsgewährung definierende vertragliche Vereinbarung gestellt werden, ist nicht ausgeschlossen, allerdings auch nicht vorgegeben. Ein Beispiel sind – sofern sie Daten zentral speichern – PIMS, die dem datenschutzrechtlich Betroffenen in ihrer Datentreuhandfunktion Zugang zu den über ihn bei Datenverarbeitern gespeicherten Daten mitteln, indem sie Betroffenenrechte ausüben. Im Falle des Einwilligungsmanagements können sie Datenverarbeitern Zugang zu Daten des Betroffenen mitteln. Auch Data-Escrows gehören zu den fakultativen Data-Hosts.

Obligatorische Datentreuhandmodelle zeichnen sich dagegen dadurch aus, dass technisch-faktische Dateninhaber gesetzlich verpflichtet werden, die Datentreuhandmodelle in bestimmten Verarbeitungssituationen zu nutzen oder ihre Daten insgesamt in die Datentreuhand auszulagern. Letzteres sollte insb. aufgrund der Gefahren für die Privatautonomie und den Geschäftsgeheimnisschutz usw. zunächst die Ausnahme bleiben, kann aber eine wichtige Lösungsoption gerade für solche Fälle sein, in denen der technisch-faktische Dateninhaber nicht der (einzig) legitime Dateninhaber ist.

Obligatorische Data-Cache-Modelle (Datendurchleitungsinstanzen) finden sich im australischen Consumer Data Right mit der Gateway Person. Ein Beispiel für einen obligatorischen Data-Host ist der im Mobilitätssektor vom Verkehrsgerichtstag vorgeschlagene Datentreuhänder, bei dem die Daten aus dem vernetzten Fahrzeug gespeichert werden.

Eine zentrale Speicherung von Daten geht tendenziell mit höheren Risiken einher als eine dezentrale Speicherung. Wenn sich eine große Menge an Daten bei einem Datentreuhänder sammelt, zentriert sich hier eine gewisse „Datenmacht“, die das Risiko des Missbrauchs birgt. Zudem ist bei Angriffen

gegen den Intermediär der potentielle Schaden höher. Die dezentrale Speicherung hat für den Dateninhaber den Vorteil, dass er die technische Kontrolle über die Daten behält. Die zentrale Speicherung beim Datentreuhänder verspricht eine einfachere, standardisierte Verwaltung der Daten durch den Datentreuhänder. Zudem kann es mitunter geboten sein, Daten zentral bei einem Datentreuhänder zu speichern, um etwa den Datenverarbeiter vom Zugang auszuschließen (Microsoft Cloud). Der Datentreuhänder wird im Falle einer zentralen Speicherung – sofern das Datentreugut nicht verschlüsselt wird – faktisch in die Lage versetzt, das Datentreugut zu nutzen (z.B. zu analysieren) oder in seiner Integrität zu verändern (z.B. zu löschen).[266] V.a. das Datenschutzrecht entscheidet derzeit darüber, inwieweit dies zulässig ist. Der Datentreuhänder könnte die Funktion übernehmen, Daten zu anonymisieren oder zu pseudonymisieren und nur die entsprechend anonymisierten oder pseudonymisierten Daten an (vertraglich definierte) Dritte herauszugeben. Ggf. bedarf es der regulatorischen Entscheidung darüber, ob und ggf. unter welchen Voraussetzungen er diese Funktion wahrnehmen darf oder als reine über den Datenzugang entscheidende Instanz ausgestaltet sein soll. Ebendies gilt für etwaige Befugnisse, Metadaten zu erstellen und/ oder zu nutzen.[267]

Wird der Begriff der Datentreuhand mit dem hier vertretenen Ansatz weit verstanden, dann lassen sich eine Reihe von Datenzugangsinfrastrukturlösungen, die bereits im Bereich des Forschungsdatenzugangs existieren, darunter fassen, so z.B. das Krebsregister aber auch die Forschungsdatenzentren.

Was bislang allerdings weitgehend inexistent ist, sind privatrechtlich organisierte freiwillige Datentreuhandmodelle, die es Forschenden ermöglichen, ihre Daten in einer sicheren Umgebung miteinander zu teilen.[268] Sie sind erforderlich, weil die bisherigen Treuhandmodelle, wie das Krebsregister, auf bestimmte Daten beschränkt sind. Nur freiwillig geschaffene Datenräume ermöglichen die Flexibilität in der Art der geteilten Daten. Z.B. ließen sich in einer solchen freiwilligen Datentreuhand Radiologiebilddaten zu Forschungszwecken teilen.[269] Auch die Data Hubs in Großbritannien sind derartige Treuhandlösungen.

Kein Datentreuhänder ist dagegen der Datenmarktplatz. Er bringt Anbieter und Nachfrager von Daten ausschließlich im Eigeninteresse zusammen, ohne die Daten selbst zu speichern. Ein Beispiel ist der Mobilitätsdatenmarktplatz („MDM-Plattform“) des Bundesverkehrsministeriums.

[266] Zur Nutzung von Information vgl. *Zech*, Information als Schutzgegenstand, 2012, S. 124 ff.
[267] Vgl. zum Begriff der Metadaten *Martini*, in: Paal/Pauly, DSGVO, 3. Auflage, 2021, Art. 30 Rn. 11.
[268] Eines der wenigen Anwendungsbeispiele für derartige freiwillige Datentreuhandmodelle ist der Dienst des Unternehmens Apheris.
[269] Specht-Riemenschneider/Radbruch, Datennutzung und -schutz in der Medizin: Forschung braucht Daten, Deutsches Ärzteblatt 118 (2021), 27, 27-28.

d) Personal Information Management Systems (PIMS)

Legt man eine weite Definition der Datentreuhand zugrunde, so fallen auch PIMS darunter, die personenbezogene Daten i.d.R. lokal speichern und es der betroffenen Person durch Voreinstellungen ermöglichen, selbstbestimmt zu entscheiden, für welche Zwecke diese Daten mit wem unter welchen Bedingungen geteilt werden sollen.[270] Sie mitteln den Unternehmen den Datenzugang und handeln dabei im Interesse des Betroffenen. Nach § 26 TTDSG können derartige PIMS im Anwendungsbereich des TTDSG anerkannt werden und dürfen sodann im Namen des Betroffenen handeln. Für Ihre Anerkennung erhalten sie insofern Rechtssicherheit in Bezug auf die Möglichkeit, datenschutzrechtliche Befugnisse für den Betroffenen ausüben zu können. PIMS können zu effektiverem Datenschutz beitragen, weil sie sowohl die datenschutzrechtliche Information unterstützen als auch die Durchsetzung des Datenschutzrechtes für die Betroffenen erleichtern und so selbstbestimmtere Entscheidungen ermöglichen können. Selbst der europäische Datenschutzbeauftragte fordert eine Förderung solcher datenschutzunterstützenden PIMS.[271] Im California Consumer Privacy Act können Verbraucherrechte über sogenannte „authorized agents" ausgeübt werden, vgl. Sect. 999.306, Sect. 999. 315 und Sect. 999.326 CCPA. Betroffene müssen die Datenverarbeitung unter dem TTDSG über PIMS aber weiterhin durch eine Einwilligung legitimieren, die, auch wenn sie gegenüber PIMS erteilt wird, einer engen Zweckbindung unterliegt.[272] Die Möglichkeit eines broad consent, wie er durch die Medizininformatik-Initiative mit den Datenschutzaufsichtsbehörden abgestimmt wurde, wäre auch für die Einwilligungserteilung gegenüber PIMS ein gangbarer Weg. Alternativ könnte das Konzept der dynamischen Einwilligung herangezogen werden: In einem ersten Schritt könnte beispielsweise vorgesehen werden, dass der Nutzer ganz grundsätzlich durch Festlegung seiner Datenschutzpräferenzen entscheiden kann, für welche breiten Zwecke er die ihn betreffenden Daten zur Verfügung stellen möchte (z.B. für Zwecke der medizinischen Krebsforschung). Für den Fall, dass eine passende Forschungsinstitution Interesse an den Daten anmeldet, könnte der Nutzer über das PIMS um seine Einwilligung für den konkreten Fall

[270] *Kollmar/El Auwad*, Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen, K&R 2021, 73, 78 mwN; vgl. auch: *Schwartmann/Benedikt/Reif*, Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz?, MMR 2021, 99, 101; *Schwartmann*/*Hanloser*/*Weiß*, PIMS im TTDSG, Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz, Kurzgutachten im Auftrag der European netID Foundation, Stiftung Datenschutz, Neue Wege bei der Einwilligung, S. 4 f., abrufbar unter: https://enid.foundation/wp-content/uploads/2021/03/Schwartmann_Hanloser_Weiss-Kurzgutachten_Dienste_zur_Einwilligungsverwaltung_20210302.pdf, zuletzt abgerufen am 16.07.2021.

[271] *European Data Protection Supervisor*, Opinion on Personal Information Management Systems, Opinion 9/2016, S. 8.

[272] *Lang*, TTDSG – Neuregelung des Datenschutzes in den Bereichen Telekommunikation und Telemedien geplant, K&R 2020, 714, 716; *Richter*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses am 24.02.2021 zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien, 2021, S. 3, abrufbar unter: https://www.bundestag.de/resource/blob/835918/ed8f50751361504905bfa51b4ee6f738/19-9-1045_Stellungnahme_SV_Richter_Stiftung_Datenschutz_oeA_TTDSG_21-04-2021-data.pdf, zuletzt abgerufen am 16.07.2021.

gebeten werden.[273] Eine dynamische Einwilligung dürfte auch mit den strengen Vorgaben des Datenschutzrechts de lege lata vereinbar sein. Erwägenswert de lege ferenda scheint aber eben auch die Aushandlung der Voraussetzungen einer breiten Einwilligung.[274]

Jeder Zugriff auf die von den PIMS gehaltenen Daten könnte protokolliert und damit nachverfolgt werden, durch staatliche Anerkennung oder Zertifizierung könnte dafür gesorgt werden, dass PIMS gewisse Mindestvoraussetzungen erfüllen.[275] Dass sie in Übereinstimmung mit geltendem Datenschutz- und IT-Sicherheitsrecht agieren müssen, ist ohnehin unbestritten. Die Regelung des § 26 TTDSG hat schon aufgrund ihres Standortes im TTDSG einen engen sachlichen Anwendungsbereich, wünschenswert wäre eine Verortung materiell-rechtlicher Vorgaben für PIMS (auch) innerhalb der DSGVO[276] oder des Data Acts. Die Vorgaben des Entwurfs des Data Governance Acts für PIMS regeln im Wesentlichen formale Anforderungen.

Im Rahmen eines Forschungsdatenzugangsgesetzes könnten PIMS die wichtige Funktion der Datenspende unterstützen.[277] Auch im Datenzugangsökosystem Australiens und Finnlands sind derartige Datenspenden vorgesehen.[278] Eine Vorbildregelung findet sich im nationalen Recht auch in § 363 SGB V. Das Konzept der Datenspende ist für die medizinische Forschung so wichtig, weil es auf große Zustimmung in der Bevölkerung trifft. Nach einer Forsa-Umfrage im Auftrag der Technologie-

---

[273] *Verbraucherzentrale Bundesverband*, Personal Information Management Systems (PIMS), 2020, S. 7, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf, zuletzt abgerufen am 16.07.2021.

[274] Dies empfiehlt im Kontext der Datenspende für medizinische Forschungszwecke auch der Deutsche Ethikrat: vgl. *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, Stellungnahme v. 30.11.2017, S. 39, abrufbar unter: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf, zuletzt abgerufen am 16.07.2021.

[275] *Specht-Riemenschneider*/*Blankertz* et al., Die Datentreuhand, MMR-Beilage 2021, S. 25, 32 f.

[276] Ähnlich *Verbraucherzentrale Bundesverband*, Datenschutz und Privatsphäre bei Telekommunikationsdiensten und Telemedien sicherstellen, Stellungnahme des Verbraucherzentrale Bundesverband im Rahmen der Anhörung des Ausschusses Wirtschaft und Energie des Deutschen Bundestags zum Gesetzentwurf für eine Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG-E) am 16.04.2021, S. 5, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2021/01/22/21-01-21_vzbv-stellungnahme_ttdsg-e.pdf, zuletzt abgerufen am 16.07.2021.

[277] Diese Vorteile einer selbstbestimmteren Entscheidung sehend auch *Assion*, Stellungnahme im Rahmen der Anhörung des Ausschusses Wirtschaft und Energie des Deutschen Bundestags zum Gesetzentwurf für eine Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG-E) am 16.04.2021, S. 10, abrufbar unter: https://www.bundestag.de/resource/blob/835498/3fc24ea374301c2ba608c9509cc64ec1/19-9-1039_Stellungnahme_SV_Assion_oeA_TTDSG_21-04-2021-data.pdf, zuletzt abgerufen am 16.07.2021; zur Datenspende vgl. *Veil*, Datenaltruismus: Wie die EU-Kommission eine gute Idee versemmelt, CR-Online Blog v. 01.12.2020, abrufbar unter https://www.cr-online.de/blog/2020/12/01/datenaltruismus-wie-die-eu-kommission-eine-gute-idee-versemmelt/, zuletzt abgerufen am 16.07.2021; zu den Chancen des Einsatzes von PIMS im Gesundheitssektor vgl. auch *Verbraucherzentrale Bundesverband*, Personal Information Management Systems (PIMS) – Chancen, Risiken und Anforderungen, Positionspapier vom 19.2.2020.

[278] Vgl. auch *Strech/von Kielmannsegg/Zenker/Krawczak/Semler*, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, 2020, S. 125 ff, abrufbar unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf, zuletzt abgerufen am 16.07.2021.

und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) sind knapp 79% der Deutschen zu einer solchen freiwilligen Datenspende bereit.[279]

[279] https://www.tmf-ev.de/zoombild.aspx?img=/Portals/0/TMF_07rz_01.jpg&text=, zuletzt abgerufen am 16.07.2021; https://www.tmf-ev.de/News/articleType/ArticleView/articleId/4456.aspx, zuletzt abgerufen am 16.07.2021.

XI. Standardisierung im Rahmen des Forschungsdatenzugangs und Datennutzung durch die Forschung

Neben der rechtlichen Eröffnung bzw. Ausgestaltung des Forschungsdatenzugangs ist für das Gelingen datenbasierter Forschungsvorhaben die Frage, in welcher Form Daten der Forschung bereitgestellt werden, zentral. Sicherzustellen gilt es dabei, dass die der Forschung zugänglich gemachten Daten auch tatsächlich von dieser gesichtet, weiterverwendet und idealerweise für das jeweilige Forschungsvorhaben nutzbar gemacht werden können. Parallel zur Schaffung von Interoperabilität ist dabei insb. die Zugänglichmachung qualitätsvoller, dokumentationsreicher und nachvollziehbarer Datenbestände sowie die Setzung von IT-Sicherheitsanforderungen bei der Bereitstellung von Daten mitzudenken. Die Festlegung auf einheitliche Datenstandards, Standards im Rahmen der Interoperabilität und der Datensicherheit einerseits, sowie auf ein definiertes Maß an Datenqualität andererseits, stehen dabei als Herausforderungen im Mittelpunkt.

1. Standardisierung als Steuerungselement im Rahmen des Forschungsdatenzugangs

Standardisierung trägt als Steuerungselement zur Vereinheitlichung unterschiedlicher Verfahrensweisen bei, an deren Ende die Etablierung eines Standards steht. Der Begriff Standard kann dabei unterschiedlich verstanden werden. Klassischerweise wird zwischen dem technischen und dem ökonomischen Standardbegriff unterschieden:

- Als technischer Standard kann eine Spezifizierung von Formaten und Protokollen verstanden werden, die darauf ausgerichtet ist, mindestens zwei Komponenten eines gemeinsamen Systems auf vorhersehbare Weise zusammenarbeiten und Daten austauschen zu lassen.[280] Technische Standards werden regelmäßig in einem formalisierten Prozess von einem rechtlich anerkannten Normungsgremium definiert.[281] Das Ergebnis wird auch als Norm oder technische Norm bezeichnet. Technische Normen werden deshalb auch als De-jure-Standard bezeichnet.[282]

- Aus der ökonomischen Perspektive ist der Begriff des „Standards“ dagegen an den allgemeinen Sprachgebrauch anzulehnen, „wonach ein Standard ein üblicher oder geforderter

[280] *Mundhenke*, Wettbewerbswirkungen von Open-Source-Software und offenen Standards auf Softwaremärkten, 2007, S. 168.
[281] Als etablierte Normungsinstitutionen auf nationaler, europäischer und internationaler Ebene seien hier hervorgehoben: Deutsches Institut für Normung (DIN), European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC), European Telecommunications Standards Institute (ETSI) sowie die International Standard Organisation (ISO).
[282] *Mundhenke*, Wettbewerbswirkungen von Open-Source-Software und offenen Standards auf Softwaremärkten, 2007, S. 168-169.

> Grad der Qualitätsmerkmale oder eine Wertstufe ist und als Referenzmaßstab für etwas zu betrachten ist, was allgemein akzeptiert und angewandt wird“ (De-facto-Standard).[283] Daraus leitet die Ökonomie ab, dass eine technische Spezifizierung sich zunächst im Wettbewerb „behaupten und im Markt durchsetzen muss, um als Standard akzeptiert zu werden“. Entscheidend ist nicht, von wem und auf welche Weise eine technische Spezifizierung formuliert wird, sondern es kommt vielmehr auf den Verbreitungsgrad im Markt an.[284]

De-facto-Standards können auch nachträglich noch von einem Standardisierungsgremium als De-jure-Standards anerkannt und zur Norm erhoben werden. Vorliegend soll die technische und die ökonomische Sichtweise grundsätzlich gleichberechtigt berücksichtigt werden. Unter einem Standard für den Forschungsdatenzugang wird im Folgenden eine technische Spezifizierung verstanden, die eine hinreichende marktliche Relevanz aufweist und das Ergebnis eines offenen, transparenten Prozesses einer Standardisierungsorganisation ist.[285]

Standardisierung (wie etwa durch DIN oder ISO-Nomen) im Rahmen datenbasierter Forschung ist dabei in drei Stadien zu denken: dem Zugang der Forschung zu Daten, der Verwendung der Daten durch die Forschung und der Nachnutzung von Forschungsdaten. Für den Forschungsdatenzugang, auf dem hier der Fokus liegt, ist daher vorwiegend die Erarbeitung von Standards für die Bereitstellung von Daten im Rahmen des Forschungsdatenzugangs zu beleuchten. Dabei sei angemerkt, dass sich die Forschung bei der Verwendung oder Nachnutzung von Daten disziplinübergreifend bereits regelmäßig innerhalb von DIN-Normen, ISO-Normen[286] oder generellen Prinzipien (wie beispielsweise den FAIR Data Principles) bewegt.

---

[283] *Mundhenke*, Wettbewerbswirkungen von Open-Source-Software und offenen Standards auf Softwaremärkten, 2007, S. 169.

[284] *Mundhenke*, Wettbewerbswirkungen von Open-Source-Software und offenen Standards auf Softwaremärkten, 2007, S. 169.

[285] Zusammenführung der Definitionen aus DIN EN 45020 und *Mundhenke*, Wettbewerbswirkungen von Open-Source-Software und offenen Standards auf Softwaremärkten, 2007, S. 169.

[286] Überwiegend sind dies Normierungen, die im Ursprung Regelungsbedarfen in der Industrie und im Dienstleistungssektor entsprechen. Für eine Liste an forschungsrelevanten DIN/ISO Normen siehe *Rat für Informationsinfrastrukturen*, Herausforderung Datenqualität - Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel, 2020, S. 17, abrufbar unter: https://rfii.de/download/herausforderung-datenqualitaet-november-2019/, zuletzt abgerufen am 16.07.2021.

Abb. 13: Stadien datenbasierter Forschungsvorhaben

Stadien datenbasierter Forschungsvorhaben		
Zugang	*Verwendung*	*Nachnutzung*
Bereitstellung von Daten für die Forschung	Nutzung von Daten im Rahmen des Forschungsvorhabens	Bereitstellung von Daten im Anschluss an das Forschungsvorhaben

2. Fachspezifische Leitlinien, Data-Policies und generelle Prinzipien zum Umgang der Forschung mit Daten

Im Rahmen der Standardisierung sind auch bereits bestehende fachspezifische Leitlinien, Data-Policies oder generelle Prinzipien (wie beispielsweise die FAIR Data Principles) miteinzubeziehen. Zumeist beinhalten diese Zielvorgaben für den fachspezifischen Binnenumgang mit Daten im Rahmen der Forschung[287] oder werden wie die FAIR-Principles v.a. zum Zwecke der Nachnutzung von Forschungsdaten diskutiert. Leitlinien, Data-Policies und generelle Prinzipien nehmen auf die Standardisierung Einfluss. So entfalten beispielsweise die FAIR Data Principles, als generelle Regelungen auch im Rahmen der Standardisierung der Datenbereitstellung eine mittelbare Relevanz, da etwa eine effektive Nachnutzbarkeit (reusability) von Forschungsdaten direkt mit der Frage, in welcher Form die Daten dem Forschenden zu Beginn seines Forschungsvorhabens bereitgestellt wurden, verbunden ist.

3. Ein Set von Standards für den Forschungsdatenzugang

Standardisierung im Rahmen des Forschungsdatenzugangs ist nicht eindimensional zu denken, sondern vielmehr als ein Mehrebenen-Set, das die Art und Weise, wie Daten der Forschung bereitgestellt werden, definiert. Hierbei ist insb. an Standardisierung im Rahmen der Interoperabilität, der Datensicherheit sowie der Datenqualität zu denken.

Abb. 14: Standardisierung im Rahmen des Forschungsdatenzugangs

[287] Bspw. die DFG Leitlinie zum Umgang mit Forschungsdaten, abrufbar unter https://www.dfg.de/download/pdf/foerderung/grundlagen_dfg_foerderung/forschungsdaten/richtlinien_forschungsdaten.pdf, zuletzt abgerufen am 16.07.2021.; eine Liste weiterer Policies und Leitlinien findet sich unter: https://www.forschungsdaten.info/themen/ethik-und-gute-wissenschaftliche-praxis/leitlinien-und-policies/, zuletzt abgerufen am 16.07.2021.

a) Interoperabilität

Unter Interoperabilität kann grundsätzlich „die Fähigkeit verschiedener Systeme, Organisationen und Techniken zusammenzuarbeiten“ verstanden werden.[288] Weiter kann nach drei Formen der Interoperabilität differenziert werden: Grundlegende Interoperabilität[289], strukturelle Interoperabilität[290] und semantische Interoperabilität. Für den Forschungsdatenzugang ist v.a. letztere Form der Interoperabilität von zentraler Bedeutung. Durch semantische Interoperabilität können Daten, die mit unterschiedlichen Kommunikationsprotokollen erfasst wurden, ausgetauscht und so von der Forschung interpretiert werden. Dazu werden neben den Daten, die Syntax (also die Spezifikationen des Datenformats/Datenstandards und der Struktur) der Daten, die gemeinsame Terminologie (Semantik), sowie auf technischer Seite Protokolle und Schnittstellen definiert sowie ggf. Metadatenstandards gesetzt, welche es ermöglichen, auch den Entstehungskontext der Daten zu berücksichtigen (siehe hierzu Ausführungen zur Datenqualität[291]). Andere Systeme können so die Bedeutung der ausgetauschten Informationen verstehen. Daraus ergeben sich vier Ebenen der Interoperabilität[292]:

[288] *Bundesregierung*, Datenstrategie der Bundesregierung, 2021, S. 113, abrufbar unter: https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1, zuletzt abgerufen am 16.07.2021.

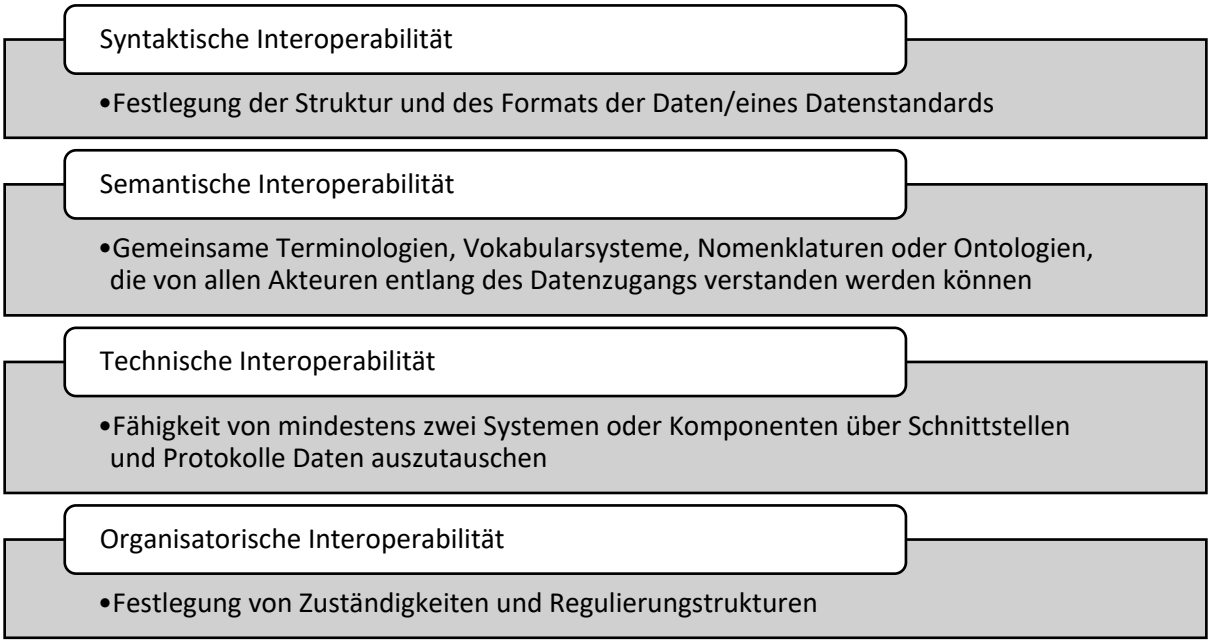
[289] Eine grundlegende Interoperabilität bedeutet, dass Systeme grundsätzlich Daten austauschen können. Da dabei jedoch keine einheitliche Standardisierung, beispielsweise zu Kommunikationsprotokollen getroffen werden, kann in den meisten Fällen die richtige Interpretation der ausgetauschten Daten durch die einzelnen Systeme nicht gewährleistet werden.

[290] Bei struktureller Interoperabilität werden die Struktur und das Format der Daten durch die Verwendung gemeinsamer Sprache oder Protokolle definiert, so dass die Bedeutung der ausgetauschten Daten interpretiert werden kann. Allerdings kann die Bedeutung der Daten, wenn sie aus unterschiedlichen Kontexten stammen, durch das Fehlen von Metainformationen unklar bleiben.

[291] X. 3. c).

[292] Angelehnt an *Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen*, Digitalisierung für Gesundheit: Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, 2021, S. 113, abrufbar unter: https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021.pdf, zuletzt abgerufen am 16.07.2021.

Abb. 15: Vier-Ebenen System der Interoperabilität



Für die Forschung erwächst die Bedeutung der Interoperabilität einerseits aus der Tatsache, dass diese im Rahmen datenbasierter Forschungsvorhaben regelmäßig Grundvoraussetzung für die Ermöglichung interdisziplinärer oder internationaler Zusammenarbeit ist. So helfen gemeinsame Standards im Rahmen der Interoperabilität dabei, fachspezifische Datensilos aufzubrechen, die aufgrund mangelnder Schnittstellen, fehlender syntaktischer Interoperabilität oder Terminologien zuvor nicht miteinander verbunden waren. Daneben generiert Standardisierung im Rahmen der Interoperabilität Rechtssicherheit bei der Bereitstellung von Daten für die Forschung. Die Etablierung semantischer Interoperabilität ist fächerübergreifend als essentieller Schlüssel für die Interpretierbarkeit von Daten durch die Forschung und die Etablierung datenintensiver Forschung anzusehen.

b) Datensicherheit

Datensicherheit bezeichnet technische und organisatorische Maßnahmen, die notwendig sind, um ein dem jeweils vorliegenden Schutzbedarf angemessenes Schutzniveau zu gewährleisten.[293] Dabei ist zwischen der zu wahrenden Datensicherheit auf Seiten der Datenbereitstellenden und auf Seiten der Forschung zu differenzieren.

Auf datenbereitstellender Seite gilt es im Rahmen des Forschungsdatenzugangs insb. Datensicherheit im Sinne eines Schutzes vor unberechtigtem Zugang, Datenveränderung und Zugangsmanipulation sicherzustellen.[294] Ist die notwendige Datensicherheit auf datenbereitstellender Seite hingegen nicht

[293] *Bundesregierung*, Datenstrategie der Bundesregierung, 2021, S. 109, abrufbar unter: https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1, zuletzt abgerufen am 16.07.2021.
[294] Vgl. https://www.wissenschaftsrat.de/download/2020/8667-20.pdf?__blob=publicationFile&v=5 S. 50

gegeben, wird auch das Vertrauen in die bereitgestellten Daten auf Seiten der Forschung sinken und datenbasierte Forschung eher gehemmt werden. Eine IT-Sicherheitszertifizierung (etwa durch das BSI) für die datenbereitstellende Seite, wie sie bereits vereinzelt im Rahmen einiger Forschungsdatenrepositorien durchgeführt wurde[295], erscheint daher für den Forschungsdatenzugang unabdingbar. Daneben hat die datenbereitstellende Seite in Abhängigkeit von der Sicherheitsrelevanz der mit der Forschung geteilten Daten, Kriterien festzulegen, die bei der Datennutzung durch die Forschung einzuhalten sind. Die festgelegten Maßnahmen für die Datensicherheit können sich dabei an einem Sicherheitskonzept des datenabfragenden Forschenden orientieren, sollten jedoch auch an der objektiven Sicherheitsrelevanz der Daten gemessen werden.

Auf Seiten der datenabfragenden Forschung ist die Erstellung eines IT-Sicherheitskonzept für die abgefragten Daten zu fordern, welches sich ebenfalls an der objektiven Sicherheitsrelevanz der Daten orientiert. Dabei ist insb. zu beachten, dass durch eine Einbindung der Forschung im Rahmen der Datensicherheit auch Vertrauen auf der datenbereitstellenden Seite in den gewissenhaften und sicheren Umgang mit den zur Verfügung gestellten Daten geschaffen wird.

c) Datenqualität

Abzugrenzen sind Standards im Rahmen der IT-Sicherheit und der Interoperabilität von Anforderungen an die Datenqualität. „Der Begriff Datenqualität bezeichnet sowohl allgemeine, beispielsweise unter Methodengesichtspunkten geforderte, typische Eigenschaften der Daten selbst als auch deren durch qualitätssichernde Maßnahmen gegebenenfalls zusätzlich geschaffene Eignung für eine weitere Nutzung.“[296] Damit adressiert der Begriff der Datenqualität die Güte von Daten. Klassische, für die Forschung sehr relevante Fragen der Datenqualität betreffen etwa die Genauigkeit von maschinengenerierten Messwerten, die Zuverlässigkeit eines empirisch gewonnenen Ergebnisses, die Aktualität von Daten oder die Dokumentation der Datengewinnung und der Datenspeicherung. Je nach Forschungsvorhaben und Fachdisziplin, kann eine hohe Datenqualität notwendige Voraussetzung für die Nutzung der Daten sein.

Im Rahmen des Forschungsdatenzugangs ist dabei nicht in erster Linie die Datenqualität zu sichern, sondern vielmehr dafür zu sorgen, dass neben den Daten genügend Zusatzinformationen (Metadaten), welche die Datenqualität der bereitgestellten Daten beschreiben, zur Verfügung gestellt werden.

[295] Vgl. *Recker*/*Helbig*/*Neumann*, Zertifizierung von Forschungsdatenrepositorien - Wege, Praxiserfahrungen und Perspektiven, Bausteine Forschungsdatenmanagement: Empfehlungen und Erfahrungsberichte für die Praxis von Forschungsdatenmanagerinnen und -managern 2020, 97, 100.
[296] *Rat für Informationsinfrastrukturen*, Herausforderung Datenqualität - Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel, 2020, S. 7, abrufbar unter: https://rfii.de/download/herausforderung-datenqualitaet-november-2019/, zuletzt abgerufen am 16.07.2021.

Metadaten sind strukturierte Daten, die Informationen über andere Daten beschreiben.[297] Diese sollten für eine Nutzbarmachung zu Forschungszwecken in Form eines zu wählenden Metadatenstandards übermittelt werden und zumindest „Auskunft über die Datengenerierung, Weiterverarbeitung sowie ggf. die verwendeten Instrumente und Methoden geben"[298].

Auch Nachhaltigkeitsaspekte können bei der Datenqualität beachtet werden. Dabei geht es insb. um Fragen der Portabilität der Daten, der Datenarchivierung oder Haltbarkeit von Datenträgern. Diese Aspekte betreffen neben der Nachnutzung von Forschungsdaten auch den Forschungsdatenzugang, da sowohl die erstmalige Nutzung von Daten zu Forschungszwecken, als auch die wiederholte Nutzung von Forschungsdaten, idealerweise vielfältige, wie auch neue Formen und Methoden der wissenschaftlichen Nutzung unterstützen sollen könnte.[299]

Inwieweit darüber hinaus Portabilitäts- oder auch Interkonnektivitätsanforderungen im Rahmen von Standardisierung auf Ebene des Forschungsdatenzugangs zu berücksichtigen sind, lässt sich nur schwer einschätzen. Im Rahmen der Verknüpfung unterschiedlicher Datenräume (z.B. im Rahmen von GAIA-X) sind technische und semantische Interkonnektivitätsanforderungen aber bereits forschungsunspezifisch thematisiert worden.[300]

4. Bestandsaufnahme Datenstandardisierung beim Forschungsdatenzugang nach Sektoren

a) Online-Wirtschaftssektor

Immer häufiger werden der Forschung auch Daten aus der Online-Wirtschaft (beispielsweise Smartphone-Nutzungsdaten oder Daten von Social-Media-Plattformen) zugänglich gemacht. Dabei geht mit dem Forschungsdatenzugang oftmals noch keine Nutzbarmachung für das Forschungsvorhaben einher, was nicht nur aber auch auf nicht bestehende Interoperabilität oder die Verwendung seltener, für die Forschung nicht auslesbarer syntaktischer Standards zurückzuführen ist.[301] Dies ist nicht nur bei der Forschung mit Daten aus gerätebasierten Messungen zu beobachten, sondern auch bei Beobachtungsdaten Dritter (beispielsweise Tracking-Daten). Soweit daher die

---

[297] *Bundesregierung*, Datenstrategie der Bundesregierung, 2021, S. 114, abrufbar unter: https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1, zuletzt abgerufen am 16.07.2021.

[298] *Rat für Informationsinfrastrukturen*, Herausforderung Datenqualität - Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel, 2020, B-3, abrufbar unter: https://rfii.de/download/herausforderung-datenqualitaet-november-2019/, zuletzt abgerufen am 16.07.2021.

[299] Dies wird insb. im Zusammenhang mit dem Einsatz von Daten-Analysetools bzw. -software im Forschungskontext relevant, siehe hierzu etwa https://www.wissenschaftsrat.de/download/2020/8667-20.pdf?__blob=publicationFile&v=5 S. 28; *Vermeir* et al., Global Access to Research Software: The Forgotten Pillar of Open Science Implementation, Global Young Academy, 2018, abrufbar unter: https://globalyoungacademy.net/wp-content/u, ploads/2018/03/18013_GYA_Report_GARS-Web.pdf, zuletzt abgerufen am 16.07.2021; *Davenport*/*Grant*/*Jones*, Data Without Software Are Just Numbers, Data Science Journal 19 (3), 2020, 1, 1–6.

[300] Das Projekt GAIA-X, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf?__blob=publicationFile&v=16, S. 11, zuletzt abgerufen am 16.07.2021.

[301] https://www.wissenschaftsrat.de/download/2020/8667-20.pdf?__blob=publicationFile&v=5 S. 24.

Metadaten (wie beispielsweise eingestellte Geräteparameter) bei der Industrie verbleiben, stehen Forschende einer „Blackbox“ gegenüber.[302]

Um auch den Mehrwert von Daten aus dem Online-Wirtschaftssektor für die Forschung zukünftig nutzbar zu machen, werden hier zunächst Standards für die Interoperabilität entlang der gesamten Datenwertschöpfungskette zu etablieren sein, wobei zu berücksichtigen ist, dass diese Bemühungen noch am Anfang stehen. Dies gilt auch für die Etablierung von Metadatenstandards in der Industrie. Mit GAIA-X, dem europäischen Projekt zur Umsetzung einer vernetzten Dateninfrastruktur, sollen erste Schritte in diese Richtung gegangen werden. So fordert die Bundesregierung den Aufbau einer europäisch getragenen Organisation, deren Aufgabe es als Mittler sein soll, eine Referenzarchitektur für den Austausch von u.a. Industriedaten zu entwickeln, Standards zu definieren sowie Kriterien für Zertifizierungen und Gütesiegel vorzugeben“.[303]

b) Gesundheitssektor

Für den Begriff der Interoperabilität findet sich speziell für den Gesundheitssektor bereits eine Definition der ISO[304], wie auch eine Legaldefinition im EU-Recht[305]. Beide Definitionen gehen dabei grundsätzlich von semantischer Interoperabilität für den Austausch von Gesundheitsdaten aus.

Um semantische Interoperabilität im Gesundheitswesen zu ermöglichen, wurden in den vergangenen Jahren insb. auf internationaler Ebene verschiedene offene Datenstandards (also Spezifikationen des Formats und der Struktur der Daten) wie beispielsweise HL7, FHIR oder DICOM entwickelt. Damit können Befunde und Behandlungsinformationen etwa durch das Krankenhaus so übermittelt werden und sind so strukturiert, dass sie in eine einrichtungsübergreifende elektronische Patientenakte sowie in lokalen Systemen anderer Leistungserbringer übernommen und weiterverwendet werden können. In Deutschland ist die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik), als eine durch Selbstverwaltung getragene Organisation, mit der Aufgabe der Schaffung von Standards für einen interoperablen Gesundheitsdatenaustausch betraut. Daneben pflegt die gematik auch das

[302] https://www.forschungsdaten-bildung.de/files/RfII-Datenqualitaet_201911.pdf
[303] Das Projekt GAIA-X, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf?__blob=publicationFile&v=16, S. 3, zuletzt abgerufen am 16.07.2021.
[304] Interoperabilität meint „die Fähigkeit zweier oder mehrerer Systeme oder Komponenten, Informationen fehlerfrei auszutauschen und die ausgetauschten Informationen auch sinnvoll nutzen zu können“ (vgl. ISO/IEEE 11073- 10101:2004 Health informatics – Point-of-care medical device communication – Part 10101: Nomenclature)
[305] Eine Legaldefinition der Interoperabilität von digitalen Daten im Gesundheitswesen findet sich in Art. 2 Nr. 26 der Verordnung (EU) 2017/745 des Europäischen Parlamentes und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates:
„Interoperabilität“ bezeichnet die Fähigkeit von zwei oder mehr Produkten – einschließlich Software – desselben Herstellers oder verschiedener Hersteller,
a) Informationen auszutauschen und die ausgetauschten Informationen für die korrekte Ausführung einer konkreten Funktion ohne Änderung des Inhalts der Daten zu nutzen und/oder
b) miteinander zu kommunizieren und/oder
c) bestimmungsgemäß zusammenzuarbeiten.

Verzeichnis für elektronische Standards im Gesundheitswesen (vesta), welches als ein Interoperabilitätsverzeichnis für von der gematik festgelegte oder anerkannte Standards dient.[306] Vor der Anerkennung eines Standards, der in das vesta eingepflegt werden soll, ist die gematik dabei gemäß § 291e Abs. 5 SGB V dazu verpflichtet, benannten Expertinnen und Experten Gelegenheit zur Stellungnahme zu geben. Als Experten sind gemäß § 291e Abs. 5 S. 2 Nr. 5 SGB V auch Vertreter aus fachlich betroffenen nationalen und internationalen Standardisierungs- und Normungsgremien hinzuzuziehen. Diese Bestrebungen sind auch für die datenintensive Forschung förderlich, da hierdurch im besten Fall internationale Standards bereits berücksichtigt werden können.

Neben der Spezifizierung des Formats und der Struktur der Daten (Standards wie FHIR) steht die Festlegung auf spezifische Terminologien, Nomenklaturen und Ontologien (Semantik). Hierbei wurden in den letzten Jahren mit SNOMED CT, LOINC, IDMP, HGNC ebenfalls Standards geschaffen. Mit der Festlegung der Medizininformatik-Initiative auf SNOMED-CT als semantischen Standard konnte dabei ein wichtiger Meilenstein für die Interoperabilität im Gesundheitswesen gelegt werden.[307] Mithilfe von SNOMED CT können unterschiedlichste Systeme bereits heute unterschiedliche medizinische Fachbegriffe (wie beispielsweise zu Krankheiten, deren Entstehungsgründen und möglichen Therapien) in einen international einheitlichen Zahlencode übersetzen. So werden Gesundheitsdaten aus unterschiedlichen Ländern zu unterschiedlichen medizinischen Fachbegriffen für die Forschung und auch die Praxis vergleichbar.

Da medizinische Daten i.d.R. als sensibel einzustufen sind, haben diese auch einen dementsprechend hohen Schutzbedarf durch IT-Sicherheitsvorkehrungen. Diese gilt es auch im Rahmen des Forschungsdatenzugangs zu gewährleisten. Angeknüpft werden könnte dabei an Zertifizierungsmodelle des BSI, wie sie bereits im Rahmen der Telematik-Infrastruktur bestehen.[308]

Im Rahmen der COVID-19-Pandemie haben sich ebenfalls unterschiedliche Initiativen herausgebildet, die sich mit dem Ziel einheitlicher Datenformate und Standards zur Interoperabilität für COVID-19-bezogene Daten und deren Zusammenführung beschäftigen (Gründung des Europäischen Fallregisters für Patientinnen und Patienten mit SARS-CoV-2-Infektion LEOSS, Entwicklung des COVID-Componenten-Standardisierungs (COCOS)-Konzepts, Aufbau einer nationalen Forschungsdatenplattform COVID-19). Grundidee ist es dabei zumeist, Anwendern, Entwicklern und

[306] Die Schaffung des vesta wurde dabei über das E-Health-Gesetz festgelegt. Eine Übersicht zu den bereits getroffenen Festlegungen und anerkannten Standards findet sich unter https://www.vesta-gematik.de/standards/, zuletzt abgerufen am 16.07.2021; Zur Auslegung des § 291e Abs. 8 S. 3 SGB V, siehe auch die Auffassung der Bundesregierung abrufbar unter: https://dserver.bundestag.de/btd/19/023/1902340.pdf, zuletzt abgerufen am 16.07.2021.

[307] https://www.aerzteblatt.de/archiv/213513/SNOMED-CT-Meilenstein-fuer-die-Standardisierung, zuletzt abgerufen am 16.07.2021.

[308] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/E-Health/Telematikinfrastruktur/telematikinfrastruktur.html, zuletzt abgerufen am 16.07.2021.

Forschenden eine Grundlage zu schaffen, mit deren Hilfe sie gemeinsam und interoperabel arbeiten können.[309]

c) Mobilitätssektor

Das Teilen von Daten aus dem Mobilitätsektor mit der Forschung gewinnt insb. im Lichte der Erforschung neuer, intelligenter Verkehrssysteme und des autonomen Fahrens an Bedeutung. Mit der Etablierung der mCloud (Open-Data-Portal des Bundesministeriums für Verkehr und digitale Infrastruktur) im Jahr 2016 und dem Mobilitätsdatenmarktplatz (MDM)[310] im Jahr 2014[311] wurden hierfür bereits Zugangsmöglichkeiten zu Daten aus dem Mobilitätssektor[312] geschaffen. Beide Portale berücksichtigen schon heute auch die Forschung beim Datenzugang.[313]

Der Datenaustausch erfolgt auf dem MDM-Portal maßgeblich über das Datenmodell (umfasst verwendete Terminologie, Datenformate, etc.) DATEX II.[314] DATEX II ist der in Europa verwendete Standard für den Austausch von Verkehrsinformationen und Verkehrsdaten. Die Entwicklung von DATEX II wurde Anfang der 90er Jahre vor dem Hintergrund der Notwendigkeit, Informationen zwischen den Verkehrszentralen der Autobahnbetreiber auszutauschen, initiiert. Bald entstand der Bedarf, diese Informationen auch für andere Service-Provider zu öffnen. Der zunehmende Umfang, in dem IVS-Dienste (Intelligente Verkehrs-Systeme) dimensioniert werden, sowie die neuen Digitalisierungsanforderungen, die sich durch selbstfahrende Autos ergeben, erfordern jedoch auch hier eine verstärkte Nutzung von Standards und fordern damit auch DATEX II entsprechend heraus. Für eine Weiterentwicklung des MDM, wie auch von DATEX-II als Datenmodell sind daher Konversions- und Harmonisierungsanstrengungen zwischen unterschiedlichen Datenstandards zu unterstützen, um auch hier einer Zersplitterung an Standards vorzubeugen.[315]

Im Rahmen der mCloud wird Datenabfragenden eine Datenexportfunktion angeboten. Diese ermöglicht es, Daten als RDF-Dateien nach der DCAT-AP.de-Spezifikation (gemeinsames deutsches

[309] https://www.bmbf.de/upload_filestore/pub/Daten_helfen_heilen.pdf, zuletzt abgerufen am 16.07.2021.
[310] Die Etablierung des MDM beruht dabei maßgeblich auf dem Aktionsplan der EU-Kommission zu Intelligenten Transportsystemen (ITS), der einen „National Access Point" für Mobilitätsdaten vorsieht. In Deutschland übernimmt der MDM die Rolle eines solchen Nationalen Zugangspunktes, abrufbar unter: https://ec.europa.eu/transport/themes/its/road/action_plan/nap_de, zuletzt abgerufen am 16.07.2021.
[311] Zur Entstehung https://www.mdm-portal.de/die-story/, zuletzt abgerufen am 16.07.2021.
[312] Übersicht welche Daten über das MDM-Portal bereitgestellt werden https://www.mdm-portal.de/der-mdm/technische-details/, zuletzt abgerufen am 16.07.2021.
[313] https://www.mdm-portal.de/der-mdm/ ; https://www.mcloud.de/web/guest/informationen, zuletzt abgerufen am 16.07.2021.
[314] Als Datenmodell enthält DATEX-II mehrere einzelne Standards.
[315] *Fraunhofer-Institut für Verkehrs- und Infrastruktursysteme IVI*, Mobility Data Spaces, 2020, S. 6-7, abrufbar unter: https://www.mobility-data-space.de/content/dam/ivi/mobility-data-space/documents/Whitepaper_Mobility_Data_Space_Web.pdf, zuletzt abgerufen am 16.07.2021.

Metadatenmodell zum Austausch von offenen Verwaltungsdaten) oder als CSV-Dateien zu exportieren.[316]

d) Energiesektor

Bestrebungen für einheitliche technische, syntaktische oder semantische Standards stehen im Energiesektor noch am Anfang. Vielversprechende Ansätze finden sich in Großbritannien im Rahmen des bereits vorgestellten YODA-Projekts. Die Standardisierung von Daten wird dabei als zentrales Element für ein digitales Energiesystem angesehen. Vorgeschlagen werden dazu offene Standards wie bspw. Open Charge Point Protocol (OCPP)[317], LF Energy[318] und als semantischer Standard Open Energy Ontology[319].

Grundsätzlich ist auch im Energiesektor jeder Datenaustauschprozess (auch mit der Forschung) vor dem Hintergrund der Datensicherheit zu betrachten. Dies hängt im Falle des Austauschs von Energiedaten maßgeblich mit der erheblichen Bedeutung für die Systemsicherheit u.a. des Energienetzes zusammen. Zum anderen ist auch der große Umfang an personenbezogenen Daten dafür verantwortlich. Dabei beinhalten neben den Regelungen des IT-Sicherheitskatalog für Netzbetreiber auch die Anforderungen für kritische Infrastruktur-Regelungen für die Datensicherheit. Daneben bestehen mit dem BDEW Whitepaper, ISO 31000, ISO 27019, ISO 62351 weitere Standards, die ebenfalls für die Datensicherheit der Energiewirtschaft entwickelt wurden.[320] 5. Anonymisierungs- und Pseudonymisierungsstandards

Für das Teilen personenbezogener Daten mit der Forschung wird unabhängig von der bisher erörterten Standardisierungsbedürftigkeit beim Forschungsdatenzugang (etwa im Rahmen der Interoperabilität), auch eine Standardisierung von Anonymisierungs- und Pseudonymisierungsverfahren an Bedeutung für die Forschung gewinnen, da hiermit eine Datenverarbeitung außerhalb des Anwendungsbereichs der DSGVO erreicht werden kann. Anknüpfend an Anonymisierungs- und Pseudonymisierungsstandards könnte dann eine gesetzliche widerlegliche Vermutung einführt werden, bei Einhaltung dieser Standards nicht im Anwendungsbereich der DSGVO zu agieren.[321]

6. Zusammenfassung und Eingliederung möglicher Standards in die vorgeschlagene Datentreuhandstruktur

316 https://www.mcloud.de/web/guest/informationen, zuletzt abgerufen am 16.07.2021.
317 https://www.openchargealliance.org/, zuletzt abgerufen am 16.07.2021.
318 https://www.lfenergy.org/, zuletzt abgerufen am 16.07.2021.
319 https://openenergy-platform.org/ontology/, zuletzt abgerufen am 16.07.2021.
320 *Deutsche Energie-Agentur*, Schnittstellen und Standards für die Digitalisierung der Energiewende, 2018, S. 43-44 mwN, abrufbar unter: https://www.dena.de/fileadmin/dena/Dokumente/Pdf/9240_Schnittstellen_und_Standards_fuer_die_Digitalisierung_der_Energiewende.pdf, zuletzt abgerufen am 16.07.2021.
321 *Specht*, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, 1040, 1046-1047.

Forschung benötigt Datenzugang, der auf einer standardisierten Bereitstellung von Daten beruht. Die tatsächliche Nutzbarmachung von Daten für die Forschung hängt dabei maßgeblich von der Interoperabilität, Datensicherheit und Datenqualität der bereitgestellten Daten ab. Für diese Bereiche erscheint die Etablierung eines Sets von Standards für die Datenbereitstellung im Rahmen des Forschungsdatenzugangs sinnvoll. Zu beachten ist dabei v.a., dass teilweise bereits Standardisierungen, Leitlinien und generelle Prinzipien für die Stadien der Verwendung von Daten durch die Forschung oder die Nachnutzung von Forschungsdaten bestehen, die es mitzudenken gilt. Unabhängig von der Standardisierung im Rahmen des Forschungsdatenzugangs sind auch Bestrebungen, Anonymisierungs- und Pseudonymisierungsverfahren zu standardisieren, zu verfolgen. Die Einhaltung und Etablierung solcher Standards könnte dabei von der hier vorgeschlagenen Datentreuhand als Mittler zwischen den Datenquellen und der Forschung sichergestellt werden.

XII. Leitlinien für den Forschungsdatenzugang de lege ferenda

Aus den Analysen des nationalen Rechtsrahmens für den Forschungsdatenzugang und der untersuchten ausländischen Rechtsordnungen lassen sich Leitlinien für einen Forschungsdatenzugang identifizieren, die im Folgenden dargelegt werden sollen.

1. Gesundheitssektor

Der Gesundheitssektor ist im Bereich des Forschungsdatenzugangs der am weitesten fortgeschrittene Sektor. Sowohl Orientierungspunkte für den Datenzugangsanspruch als auch für die Datenzugangsinfrastruktur (nachfolgend Unterpunkte a - j) lassen sich definieren. Daraus lässt sich letztlich ein Forschungsdatenzugangsökosystem (nachfolgend Unterpunkt k) entwickeln und in einem Gesundheitsforschungsdatenzugangsgesetz rechtlich ausgestalten (nachfolgend Unterpunkt l).

a) System originärer Forschungsklauseln normieren

Im Gesundheitssektor empfiehlt sich ein System originärer Forschungsklauseln, solcher Forschungsklauseln also, die unabhängig von möglichen bereits existenten Zugangsansprüchen anderer Akteure den Forschungsdatenzugang für die Wissenschaft originär normieren.

b) Zugang zu den Daten privater und öffentlicher Stellen durch mittelbare Datenzugangsstrukturen in staatlicher Organisation vorsehen

aa) Einspeisung privater und öffentlich gehaltener Daten ermöglichen

Forschungsdatenzugang ist bislang im Wesentlichen gegen staatliche Stellen gerichtet, dies gilt sowohl in Deutschland, wo ein Datenzugang im Gesundheitssektor v.a. Krebsregister und Forschungsdatenzentren betrifft, als auch für die untersuchten Rechtsordnungen in Finnland, Frankreich und Australien. In Großbritannien werden die Research Data Hubs von Health Data Research UK, einer unabhängigen, eingetragenen Wohltätigkeitsorganisation getragen, auch hier existiert aber kein direkter Datenzugangsanspruch gegen private Anbieter von Gesundheitsdienstleistungen. In Indien mittelt ebenfalls eine staatliche oder Non-Profit Organisation den Zugang zu den Daten Privater. Daten Privater werden aber sowohl nach nationalem Recht als auch in einigen der untersuchten fremden Rechtsordnungen in die verschiedenen Data Hubs eingespeist, z.B. in das Forschungsdatenzentrum am BfArM und in die Krebsregister der Länder, in Finnland in die Datenzugangsbehörde „Findata“, in Großbritannien in die Research Data Hubs, in Frankreich in die „Health Data Hub“ und in Australien in das „My Health Record System“. Es besteht damit ein mittelbarer Datenzugang auch zu den von Privaten gehaltenen Daten, wobei der (potentiell hohe)

Aufwand der Zugangsentscheidung und Zugangsgewährung im Wesentlichen auf öffentliche Stellen (z.B. Forschungsdatenzentrum und Krebsregister) ausgelagert wird. Ein solches System mittelbarer Zugangsstrukturen zu Daten privater und öffentlicher Stellen empfiehlt sich für den Gesundheitssektor, weil es den Aufwand für die privaten Anbieter geringhält, Verfahren vereinheitlicht und gleichzeitig private Daten in die Zugangsstrukturen einbindet.

bb) Gemischtes System zentraler, dezentral-zentraler und gänzlich dezentraler Datenspeicherarchitekturen vorsehen

Dabei müssen aber nicht alle Daten automatisiert in zentrale Daten-Hubs eingespeist werden. Vorzugswürdig erscheint vielmehr ein gemischtes System aus mehreren datenspezifischen Daten-Hubs: Daten bestimmter Krankheitsbilder sollten für den Fall der Notwendigkeit einer Zusammenführung auch zusammengeführt werden, dies muss aber nicht zwingend in einer zentralen, sondern kann auch in mehreren Forschungsdaten-Hubs geschehen (dezentral-zentrale Datenspeicherung), z.B. wie im Falle der Zusammenführung von Daten über Krebserkrankungen in den Landeskrebsregistern. Gleiches ist für Daten über asthmatische Erkrankungen oder psychische Erkrankungen in neu einzurichtende Forschungsdaten-Hubs möglich. Auch die Register der Unfall- und Rentenversicherung ließen sich als Forschungsdaten-Hubs in das System einbeziehen, um eine Zusammenführung der Daten auf Anforderung von Wissenschaft und Forschung, z.B. zur Erforschung von Zusammenhängen zwischen chronischen Erkrankungen und einem erhöhten Risiko für Stürze und Knochenbrüche, zu ermöglichen. Die Datenspezifität ist mit den Health Research Data Hubs Großbritanniens vergleichbar. Gänzlich dezentral vorzuhalten und daher nicht per se in den Forschungsdaten-Hubs zu erfassen sein sollten Daten z.B. von Wearables und Gesundheits-Apps, die erst auf Anforderung einer zentralen Koordinierungsstelle zusammengestellt und an den Antragsteller übermittelt werden. Wie wichtig die Einbindung von Wearables und Gesundheits-Apps auf Basis einer freiwilligen Entscheidung des Betroffenen ist, zeigen neuere Untersuchungen aus den USA, die belegen, dass z.B. langfristige Auswirkungen einer Covid-19 Erkrankung über die Apple Watch, Fitbit oder andere Wearables mit Blutdrucksensor erkannt werden können.[322]

Gegenüber einem System rein dezentral gehaltener Daten ist die Etablierung mehrerer datenspezifischer dezentral-zentraler Daten-Hubs wünschenswert, um beispielsweise symptomspezifische Suchanfragen vereinfacht durchführen zu können (hatten etwa Patienten mit psychischen Erkrankungen in einem bestimmten Alter auch körperliche Symptome von denen auf die psychische Erkrankung rückgeschlossen werden könnte und wenn ja, welche?). Die spezifizierten

[322] *Schesswendter*, Apple Watch und Fitbit: Wearables können Auswirkungen von Covid-19 erfassen, abrufbar unter: https://t3n.de/news/apple-watch-fitbit-wearables-corona-covid-19-long-folgen-1390278/, zuletzt abgerufen am 16.07.2021.

Daten, die jeweils in den einzelnen Daten-Hubs gespeichert werden, sind zu vergleichen mit der Speicherung eines Auszugs aus der Krankenakte des Patienten. Die dezentral-zentrale Speicherung in (z.B. Landes-)Forschungsdatenhubs verringert das datenschutzrechtliche ebenso wie das IT-sicherheitsrechtliche Risiko für die Betroffenen im Vergleich zu einer zentralen Speicherung sämtlicher Daten an einer Stelle und findet in den Landeskrebsregistern ein auch datenschutzrechtlich tragfähiges Vorbild, solange die technische Absicherung des Hubs auf höchstem Niveau gewährleistet ist. Gleichzeitig erhöht ein System mehrerer Datenspeicherstellen, die zudem dezentral in den Bundesländern eingerichtet werden, den Aufwand und damit die Kosten der Datenzugangsgewährung. Das System verschiedener Data Hubs sollte insofern mit einer zentralen Koordinationsstelle, die über den Datenzugang entscheidet, verbunden werden. In Deutschland könnten die bereits bestehenden Forschungsdatenzentren und Krebsregister unabhängig davon, ob sie als zentrale Einheit bundesweit gewährleistet werden, oder föderalen Strukturen der Länder unterliegen, als Forschungsdaten-Hubs fungieren.

cc) Datenspende, Einbindung von PIMS ermöglichen

Liegen die von den Privaten gehaltenen Daten im Gemeininteresse, weil etwa die Forschung mit Ihnen einen erheblichen Mehrwert für die Gesellschaft hätte, so ließe sich der mittelbare Zugang zu den Daten Privater noch ausbauen, etwa indem Gesundheitsdiensteanbieter weitreichender als bislang zur Bereitstellung der von ihnen erhobenen Daten über eine zentrale Datenzugangseinheit verpflichtet werden. Handelt es sich um personenbezogene Daten, so muss dies in Übereinstimmung mit dem Datenschutzrecht geschehen. Vorzugswürdig ist eine Weitergabe dieser Daten mit Einwilligung des Betroffenen und lediglich auf Anforderung der zentralen Koordinierungsstelle. Ihre im Grundsatz dezentrale Speicherung bleibt also erhalten, sie werden nicht ohne Weiteres in die Forschungsdaten-Hubs überführt, sondern allein dann, wenn der Betroffene dies wünscht. Eine wichtige Rolle könnten hier PIMS übernehmen. Diese Systeme geben Betroffenen die Möglichkeit, die sie betreffenden personenbezogenen Daten in sicheren, lokalen oder Online-Speichersystemen zu verwalten und sie zu teilen, wann und mit wem sie es wünschen. Durch eine weite Definition der Gesundheitsdiensteanbieter als alle Diensteanbieter, die Gesundheitsdaten verarbeiten, könnten auch sie unter diesen Begriff fallen und als Mittler freiwilliger Datenspenden auf Grundlage informierter Einwilligungen dienen. Auch ohne die Einbindung von PIMS kann und sollte eine Datenspende aber möglich sein; § 363 SGB V ließe sich zu diesem Zweck in seinem Anwendungsbereich erweitern.

dd) Datenstandards vorsehen und Schnittstellen vereinheitlichen

Sowohl für die Übermittlung von Daten in Forschungsdaten-Hubs als auch für die Übermittlung dezentral gehaltener Daten auf Anforderung der Koordinierungsstelle sind insbesondere semantische Standards erforderlich.

c) Anspruchsberechtigung weit, Zweckbindung gemeinwohlorientiert fassen

De lege lata bezieht sich die Anspruchsberechtigung in § 303e SGB V auf Einrichtungen der Gesundheitsversorgungsforschung, Hochschulen, Hochschulkliniken und außeruniversitäre Forschungseinrichtungen wie Fraunhofer-Gesellschaft, Helmholtz-Gemeinschaft, Leibnitz-Gemeinschaft und Max-Planck-Gesellschaft. Im Krebsregistergesetz sind allerdings ebenso Privatpersonen anspruchsberechtigt. Im finnischen Secondary Use Act ist der Kreis der Anspruchsberechtigten ebenfalls weit und bezieht sich auf alle Personen, die ihre Forschungsfreiheit ausüben. In Frankreich sind Wissenschaft und Forschung ebenfalls pauschal anspruchsberechtigt, es ist allerdings eine Zweckbindung an Forschung und Wissenschaft im öffentlichen Interesse vorgesehen. In Großbritannien ist der Kreis der Anspruchsberechtigten nicht spezifiziert und damit denkbar weit, das Risiko für die Rechte und Interessen der Betroffenen wird aber dadurch minimiert, dass eine Datenweitergabe in der Regel anonymisiert oder mit Einwilligung des Betroffenen erfolgt. In Australien ist der Kreis der Zugangsberechtigten negativ beschränkt: Vom Zugangsanspruch ausgeschlossen sind Versicherungen. Ein Datenzugang muss außerdem für die Zwecke von Wissenschaft und Forschung erfolgen.

Sind von einem Datenzugangsanspruch auch Private betroffen, so geht dieser Anspruch mit einer Einschränkung ihrer Grundrechte einher. Er muss daher verhältnismäßig sein. Dafür kommt es weniger darauf an, wer datenzugangsberechtigt ist als auf den Zweck des Datenzugangsanspruchs. Je stärker dieser Gemeinwohlinteressen dient, desto eher lässt sich ein Datenzugangsanspruch rechtfertigen. Bei der regulatorischen Ausgestaltung von Datenzugangsansprüchen sollte daher in der Regel eine enge Zweckbindung an gemeinwohlorientierte Forschung normiert werden. Ist dies der Fall, muss der Kreis der Datenzugangsberechtigten nicht auf die nicht-kommerzielle Forschung beschränkt werden. (Unions-)grundrechtlich ist Forschung jede Tätigkeit mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen,[323] ohne dass eine Beschränkung auf eine nicht-kommerzielle Forschung stattfindet.[324] Auch grundrechtsdogmatisch ließe sich die kommerzielle Forschung also in der Anspruchsberechtigung erfassen.

Das Gemeinwohlinteresse ließe sich beispielsweise in Anlehnung an das Verständnis des SGB VIII definieren als Tätigkeit, deren Erbringung nicht allein durch individuelle – wirtschaftliche,

[323] *Jarass*, in: Jarass, EU-Grundrechte-Charta, 4. Auflage, 2021, Art. 13 Rn. 8 mwN.
[324] *Bernsdorff*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage, 2019, Art. 13 Rn. 14.

eigennützige, freundschaftliche oder familiäre – Ziele motiviert ist, sondern sich zumindest auch als Ausdruck gesellschaftlicher Verantwortung erweist.[325]

Ein Forschungsdatenzugang ist mit Verantwortung hinsichtlich der zur Verfügung gestellten Daten verbunden. Ein Missbrauch ist v.a. im Betroffeneninteresse unbedingt zu verhindern. Das Bedürfnis, im Gemeinwohlinteresse einen möglichst breiten Kreis an zugangsberechtigten Forschern zu gewährleisten und das mindestens gleichgewichtige Interesse an einer Verhinderung von Datenmissbrauch ließe sich im Rahmen der Anspruchsberechtigung auflösen, indem der Kreis der Zugangsberechtigten zunächst auf Wissenschaft und Forschung insgesamt festgelegt wird, die Zweckbindung an die Gemeinwohlorientierung der wissenschaftlichen Forschung aber bereits bei Antragstellung umfassend darzulegen und zu beweisen ist. Für Forscher, die an Einrichtungen der Gesundheitsversorgungsforschung, Hochschulen, Hochschulkliniken und außeruniversitäre Forschungseinrichtungen tätig sind, könnte im Rahmen eines solchen Datenzugangskonzeptes dann wiederum widerleglich vermutet werden, dass diese gemeinwohlorientierte wissenschaftliche Forschung betreiben. Sowohl für die öffentlich finanzierte wie auch die privat finanzierte Forschung sollte es zur Voraussetzung für das Gemeinwohlinteresse gemacht werden, dass die Forschungsergebnisse der Öffentlichkeit in anonymisierter Form zugänglich gemacht werden. Die Gesetzesbegründung zu § 5a NetzDG enthält eine ähnliche Vorgabe.

Eine derart enge Fassung der Anspruchsberechtigung, wie sie in Kanada vorgesehen ist, wäre im Falle einer solchen Sicherung der Gemeinwohlorientierung durch die Zweckbindung nicht erforderlich. Übernommen werden sollte aber die negative Beschränkung des Kreises der Anspruchsberechtigten aus Australien. Das Risiko, dass die Daten hier zu Zwecken der stärkeren Personalisierung von Versicherungstarifen genutzt werden, ist so erheblich, dass sie per se von einer Anspruchsberechtigung ausgeschlossen werden sollten.

d) Zusätzliche Voraussetzungen von Datenzugang und Datenzugangsantrag vorsehen

aa) Erforderlichkeitskriterium entfallen lassen

Das in einer Reihe nationaler Forschungsklauseln vorgesehene Erforderlichkeitskriterium des Datenzugangs macht insb. dort Sinn, wo Ansprüche unmittelbar gegen private Stellen gerichtet sind, weil der Datenzugang dann regelmäßig mit einem hohen Aufwand der privaten Stelle einhergeht, der sie nicht über Gebühr belasten darf. Verwaltet aber eine Zentralstelle den Datenzugang, entstehen die Kosten für die Privaten bereits bei Einspeisung der Daten in das Datenzugangsökosystem. Hier ist durch geeignete Mechanismen (z.B. durch die Vorgabe von Schnittstellen und Datenstandards sowie Hilfestellung bei der Einspeisung der Daten) zur Kostenreduktion beizutragen. Das Kriterium der

[325] Trésoret, in: jurisPK-SGB VIII, 2. Auflage, 2018, Rn. 56; BeckOGK-*Janda*, 1.6.2021, SGB VIII § 73 Rn. 15, 16.

Erforderlichkeit muss dann aber nicht mehr für die Entscheidung des Zugangs zu diesen bereits in das System eingespeisten Daten vorgesehen werden.

bb) Schutzkonzept verlangen

Im Interesse des Schutzes von Drittinteressen sollte ein Schutzkonzept verlangt werden, und zwar unabhängig davon, ob die Daten anonymisiert oder personenbezogen übermittelt werden. Denn auch im Falle einer Anonymisierung der Daten verbleibt das Risiko einer De-Anonymisierung. Das Erfordernis eines Risiko-Management-Plans findet sich z.B. in Australien, in Kanada sowie im nationalen Recht für den Online-Wirtschaftssektor in § 5a NetzDG. An dieser Norm sollte die konkrete Formulierung des Gesetzestextes orientiert werden.

cc) Übermittlung des Datenzugangsantrags standardisieren

Für den Datenzugangsantrag sollte im Interesse einer effektiven Gewährleistung des Datenzugangs ein standardisiertes - idealerweise international einheitliches - Verfahren vorgesehen werden. Kanada, Finnland und Großbritannien beispielsweise ermöglichen die Antragstellung über ein „data request management system".

dd) Einbindung von Research Ethics Board (REB) und Data Governance Board (DaGoB) vorsehen

Es empfiehlt sich außerdem die in einigen ausländischen Rechtsordnungen (Frankreich, Finnland, Kanada, Australien) vorgesehene Einbindung einer Instanz, die über die ethische Vereinbarkeit der Forschung entscheidet. Zusätzliche Antragsvoraussetzung sollte die positive Prüfung durch dieses Research Ethics Board (REB) sein. In Kanada entscheidet diese Instanz auch und gerade darüber, ob die Daten „for approved data purposes" genutzt werden. Diese Funktion wird in Australien von dem Data Governance Board vorgenommen. Es scheint eine Trennung zwischen diesen beiden Instanzen sinnvoll, denn die Entscheidung über die ethische Vereinbarkeit des Forschungsvorhabens sollte primär durch Ethiker getroffen werden, während die Prüfung, ob die Forschung den vorausgesetzten Gemeinwohlinteressen dient, eine juristische Frage ist.

e) Regelung der Anschlussnutzung klar definieren

§ 303e SGB V unterstellt die Weitergabe der vom Zugangsanspruch betroffenen Daten einem Genehmigungsvorbehalt des Forschungsdatenzentrums. Auch datenschutzrechtlich ist die Weitergabe der Daten, die einen Verarbeitungsvorgang darstellt, dem Verbotsprinzip unterworfen. Eine zweckändernde Nutzung der Daten zu Zwecken der Wissenschaft und Forschung ist dank Privilegierung möglich, Art. 5 Abs. 1 lit. b) DSGVO. Das Krebsregistergesetz normiert, dass die Daten nur im Rahmen der zur Verfügung gestellten Zwecke genutzt werden dürfen. Sie sind frühestmöglich

zu pseudonymisieren oder zu löschen. Werden die Daten länger als fünf Jahre gespeichert, ist der Patient darauf hinzuweisen. In Frankreich ist eine Nutzung der Daten zu kommerziellen Werbezwecken untersagt, die Daten dürfen nicht verkauft werden, anonymisierte Daten dürfen nicht de-anonymisiert werden. Sämtliche dieser Einschränkungen scheinen sinnvoll, wobei das Verbot der De-Anonymisierung auch strafrechtlich adressiert werden sollte.[326] Gleichzeitig sind im Interesse von Rechtsklarheit und zur Wahrung des Bestimmtheitsgebotes Standards zur Anonymisierung vorzusehen.[327] Die in Finnland vorgesehene Pflicht zur Anonymisierung der Ergebnisse der Datenauswertung ließe sich nach Bestimmung von Anonymisierungsstandards ebenfalls vorsehen. Die in Australien untersagte Anschlussnutzung für Zwecke von Versicherungen und Arbeitgebern scheint geboten, allerdings ließe sich auch darüber nachdenken, die Anschlussnutzung durch ein Verbot der Weitergabe der Daten insgesamt restriktiv auszugestalten. Dies würde das Risiko einer missbräuchlichen Verwendung senken, weshalb der Datenzugangsanspruch zugunsten von Forschung und Wissenschaft im Sinne des Five Safes Models weitreichender ausfallen dürfte als im Falle der Zulässigkeit einer Forschungsdatenweitergabe.

Der Datenzugang durch öffentliche Stellen ließe sich als Verwaltungsakt ausgestalten. Entsprechend könnte der Forschungsdatenzugang an Auflagen und Bedingungen geknüpft und bei Verstößen widerrufen werden. Ein Verstoß gegen Vorgaben zur Anschlussnutzung sollte außerdem mit dem zeitweisen Entzug der Antragsberechtigung sanktioniert werden.

f) Schranken des Datenzugangs rechtlich und technisch vorsehen

Datenzugangsansprüche sollten im Interesse eines angemessenen Ausgleichs zwischen potentiell betroffenen Rechten und Interessen nicht unbeschränkt gewährleistet werden, sondern von entgegenstehenden Rechten und Interessen Dritter beschränkt werden. Dies kann im Gesundheitssektor insb. das informationelle Selbstbestimmungsrecht der Betroffenen sein. Zum Ausgleich zwischen Forschungsfreiheit und Informationellem Selbstbestimmungsrecht könnten die Daten entweder nur anonymisiert oder nur mit Einwilligung des Betroffenen zur Verfügung gestellt werden und/oder es könnte ein Forschungsdatenzugang innerhalb einer geschützten Infrastruktur gewährt werden, d.h. an (virtuellen) Arbeitsplätzen der Datenzugangsinstanz.

g) Vergütungsregelungen auf eine Kostendeckung der Verwaltungstätigkeit beschränken

[326] *Specht*, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, 1040, 1046-1047; *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, S. 132, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 16.07.2021.
[327] *Specht*, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, 1040, 1046-1047.

Vergütungsregelungen sind bislang in den untersuchten ausländischen Rechtsordnungen nur rudimentär ausgestaltet. In Großbritannien darf eine „Kostendeckung“ vorgesehen werden, in Finnland ist einzig vorgesehen, für welche Tätigkeiten (Zugangsentscheidung, Bereitstellung der Daten, Nutzung der sicheren Umgebung etc.) eine Gebühr erhoben werden darf, nicht aber in welcher Höhe. An dieser Regelung kann sich daher zwar grundsätzlich, nicht aber im Hinblick auf die Höhe der Vergütung orientiert werden. Auch in Frankreich ist die Festlegung einer für den Datenzugang zu erhebenden Vergütung Gegenstand eines Reflektionsprozesses bis 2022 und in Indien finden sich lediglich Angaben, dass eine Vergütung erhoben werden darf, nicht aber in welcher Höhe. Auch auf Vergütungsregelungen beispielsweise aus dem Online-Wirtschaftssektor, etwa § 5a NetzDG, der eine sehr konkrete Obergrenze der Vergütung vorsieht, kann nicht zurückgegriffen werden, weil mit dieser Vergütung der Aufwand der Privatunternehmen für den Datenzugang entschädigt werden soll. Dieser Aufwand entsteht im hier modellierten Datenzugangsökosystem den privaten Stellen aber vorgelagert bei Einspeisung Ihrer Daten, weshalb bereits an dieser Stelle unterstützt werden sollte (s.o.). Für die Zugangsgewährung durch eine öffentliche Datenzugangsstelle sollten allein die anfallenden Verwaltungskosten kompensiert werden können, um die Effektivität des Datenzugangsanspruches nicht zu gefährden. Eine umfassende Regelung der Datenzugangsvergütung für diesen Fall findet sich in der Datentransparenz-Gebührenverordnung, die für die Datenzugangsgewährung nach den §§ 303a ff. SGB V gilt. Da die Regelungen des §§ 303a ff. SGB V eine ähnliche Datenzugangsstruktur vorsehen, ließe sich auf die Regelungen der Datentransparenz-Gebührenverordnung auch für die Vergütung im hier entwickelten Datenzugangsökosystem zurückgreifen.

h) Frist hinreichend flexibel ausgestalten

Fristenregelungen im Verwaltungsbereich sollten stets einhergehen mit einer ausreichenden Personal- und Sachmitteldeckung. Gleichzeitig muss eine sorgfältige Prüfung des Datenzugangs gewährleistet sein. Flexible Fristenregelungen mit einer Obergrenze sind daher starren Fristenregelungen, die nicht oder nur unzureichend auf den konkreten Bearbeitungsaufwand reagieren können, vorzuziehen. Aus dem nationalen Recht ergeben sich hier keine Orientierungspunkte. Finnland sieht im Secondary Use Act allerdings vor, dass die Entscheidung über einen data-permit unverzüglich zu treffen ist, spätestens aber 3 Monate nach Eingang des vollständigen Antrags bei der Behörde. Eine Verlängerung ist im Einzelfall möglich. An dieser Regelung sollte sich orientiert werden.

i) Rechtsdurchsetzung und Beweislast mitdenken

Entscheidungen über den Datenzugang ergehen in der Form des Verwaltungsaktes. Der statthafte Rechtsweg für den Fall eines ablehnenden Bescheides ist daher die Verpflichtungsklage gerichtet auf den Erlass eines stattgebenden Verwaltungsaktes. Es gelten die allgemeinen Beweislastregelungen,

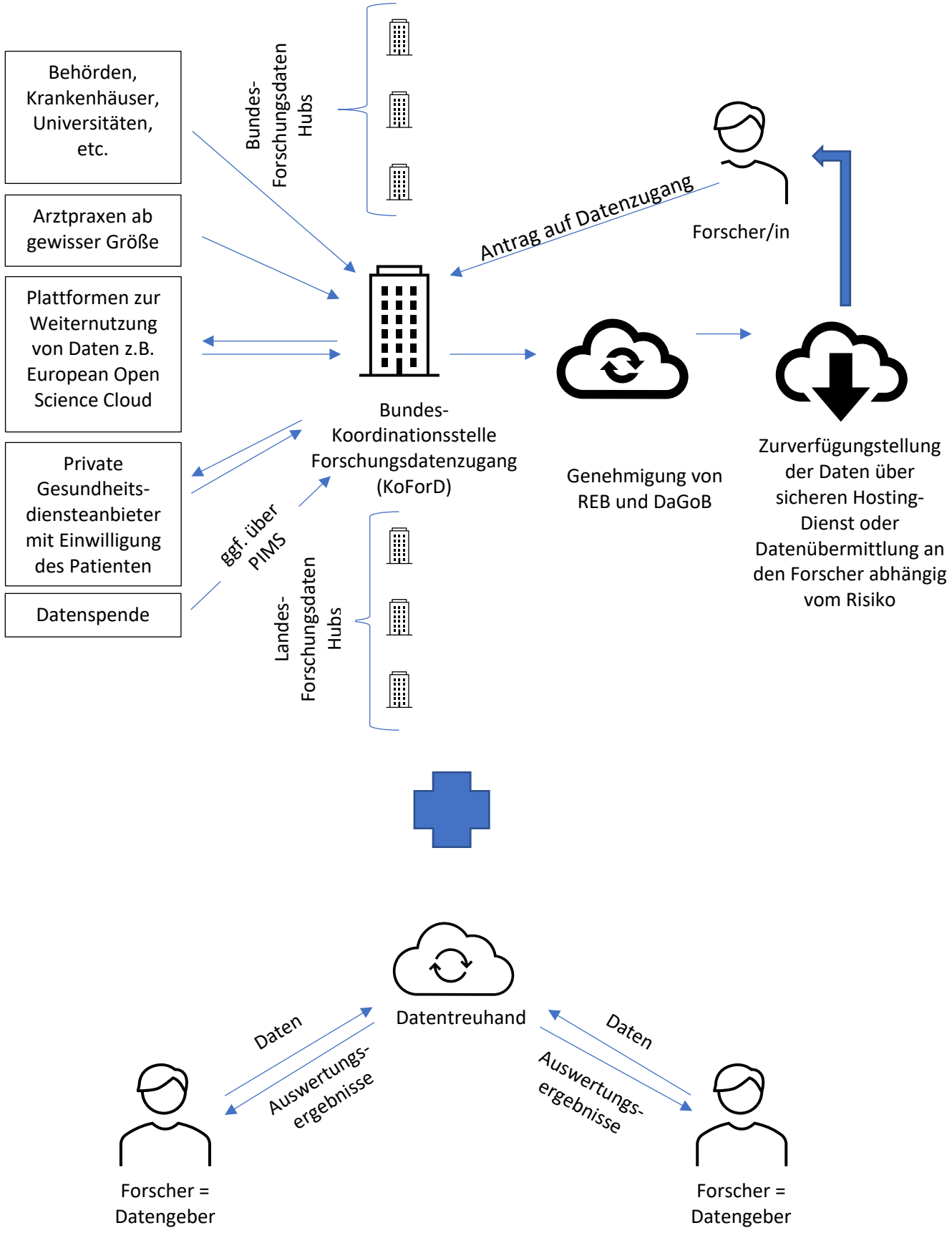
mit Ausnahme der Vermutungsregelung für das Gemeinwohlinteresse, wenn die Forschung an öffentlichen Forschungseinrichtungen im o.g. Sinne erbracht und die Forschungsergebnisse der Öffentlichkeit zugänglich gemacht werden.

j) Parallel flexible Datentreuhandstrukturen als Teil eines umfassenden Datenzugangsökosystems auf rechtssichere Grundlage stellen

Die Einrichtung einer zentralen Koordinierungsstelle sowie einer Vielzahl an Forschungsdaten-Hubs kann sich jeweils nur auf spezifische Daten beziehen. Sollen darüber hinaus vertikal verteilte Daten (bspw. unterschiedliche Daten derselben Personengruppe, die an unterschiedlichen Orten - z.B. verschiedenen Krankenhäusern - gespeichert sind) aggregiert ausgewertet werden, beispielsweise zu Zwecken der Covid-19-Nebenwirkungsforschung, sind zusätzlich zu dem entworfenen Datenzugangsökosystem flexible Datentreuhandstrukturen (wird auch als Data Clean Room bezeichnet) vorzusehen. Denn die Auswertung vertikal verteilter Daten gelingt sehr viel besser in derartigen Data Clean Rooms. Ziel muss es sein, durch Gewährleistung IT-sicherheitsrechtlich höchster Standards einen sicheren Raum zur Auswertung aggregierter Datenbestände zu schaffen und diese aggregierte Datenauswertung auf eine datenschutzrechtlich sichere Rechtsgrundlage zu stellen. Auch derzeit ist die Aggregation und Auswertung von Datenbeständen datenschutzrechtlich möglich auf Grundlage einer ausdrücklichen Einwilligung des/der Patientin (Art. 9 Abs. 2 lit. a DSGVO) sowie auf Grundlage eines überwiegenden Interesses, Art. 9 Abs. 2 lit. j) DSGVO i.V.m. § 27 BDSG (s.o.). Beide Rechtsgrundlagen bringen für den Fall der Auswertung großer Datenbestände aber eine ganz erhebliche Rechtsunsicherheit mit sich. Werden an Datentreuhandstrukturen hohe Anforderungen mit Blick auf die IT-Sicherheit gestellt, wird eine Weitergabe der Rohdaten untersagt und unter Strafe gestellt, sind die auszuwertenden Daten technisch und strafrechtlich bereits so geschützt, dass das Risiko für die Rechte und Interessen der Betroffenen minimiert ist. Sofern diese Anforderungen an die Datentreuhand erfüllt sind, sollte die aggregierte Datenauswertung innerhalb der von der Datentrauhand angebotenen Strukturen daher durch einen datenschutzrechtlichen Erlaubnistatbestand gestattet werden. Die Datentreuhand hat datenschutzrechtlich den Vorteil, dass die Daten allein in der sicheren Umgebung der Datentreuhand und nicht tatsächlich mit allen anderen Datengebern geteilt werden müssen. Geteilt werden allein die Auswertungsergebnisse, während die ausgewerteten Datenbestände in der Treuhand nach dem Auswertungsvorgang wieder gelöscht werden. Es existiert kein Anspruch Dritter auf Zugang zu den in der Datentreuhand gespeicherten Daten, die Datentreuhand ist vielmehr allein die Infrastrukturlösung zum risikoarmen Teilen und Auswerten großer Datenbestände. Auch ein Federated Learning, das einen zentralen Server verwendet, um die verschiedenen Schritte der Algorithmen zu orchestrieren und alle teilnehmenden Knoten während des Lernprozesses zu koordinieren, benötigt eine Zentralstelle und sollte in der hier beschriebenen Datentreuhand möglich sein.

k) Visualisierung des empfohlenen Datenzugangsökosystems

Abb. 16: Empfohlenes Datenzugangsökosystem im Gesundheitssektor



I) Vorschlag eines Gesundheitsforschungsdatenzugangsgesetzes

Diese Erkenntnisse für ein Datenzugangsökosystem im Gesundheitssektor lassen sich in einem Gesundheitsforschungsdatenzugangsgesetz (GFDZG) niederlegen:

§ 1 Anwendungsbereich

[1]Dieses Gesetz regelt den Zugang von Forschung und Wissenschaft zu Gesundheitsdaten. [2]Die Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (DSGVO) bleiben unberührt.

§ 2 Definitionen

Im Sinne dieses Gesetzes bezeichnet der Ausdruck

1. Personenbezogene Daten: Daten i.S.d. Art. 4 Nr. 1 DSGVO.
2. Gesundheitsdaten: Daten i.S.d. ErwGr. 35 DSGVO.
3. Nicht-personenbezogene Daten: Daten, deren Personenbezug durch Anonymisierung beseitigt wurde oder die zu keinem Zeitpunkt personenbezogen i.S.d. Art. 4 Nr. 1 DSGVO waren.
4. Anonymisierung: Die dauerhafte Beseitigung des Personenbezugs i.S.d. § 11 dieses Gesetzes
5. Broad Consent: Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung, möglichst auf Grundlage eines Mustertext zur Einholung von Patienteneinwilligungen mit breiter Forschungszweckbestimmung für die Verarbeitung pseudonymisierter Gesundheitsdaten, dem die Datenschutzkonferenz oder der Europäische Datenschutzausschuss zugestimmt hat.
6. Wissenschaft und Forschung: Jede Tätigkeit einer natürlichen Person oder einer Hochschule, einer nach landesrechtlichen Vorschriften anerkannten Hochschulklinik, einer öffentlich geförderten außeruniversitären Forschungseinrichtung oder einer sonstigen Einrichtung mit der Aufgabe wissenschaftlicher Forschung, mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen.
7. Datenzugang: Die Bereitstellung von Daten an Wissenschaft und Forschung durch Übermittlung oder durch Zugangsgewährung über einen geschützten Arbeitsplatz an der Koordinierungsstelle für den Forschungsdatenzugang (KoForD).
8. Datenzubringer: Datenverarbeiter aus dem Gesundheitssektor, d.h. Behörden, Universitäten, Privat-Kliniken, Ärzte, öffentlich eingerichtete Datenspeicher sowie Gesundheitsdiensteanbieter, die Daten an die KoForD übermitteln. Die Bundesregierung kann durch Rechtsverordnung mit Zustimmung des Bundestages und des Bundesrates den Kreis der Datenzubringer erweitern.
9. Gesundheitsdiensteanbieter: Alle Anbieter von Diensten, die Gesundheitsdaten verarbeiten.
10. Personal Information Management Systems: Systeme zur Einwilligungsverwaltung und zur Ausübung der Betroffenenrechte

11. Datentreuhand: Eine natürliche oder juristische Person oder eine Personengesellschaft, die den Zugang zu von Datentreugebern bereitgestellten oder bereitgehaltenen Daten nach vertraglich vereinbarten oder gesetzlich vorgegebenen Regelungen zumindest auch im Fremdinteresse mittelt.
12. Datengeber: Natürliche oder juristische Personen, die Daten zum Zwecke der Auswertung an eine Datentreuhand übermitteln.

§ 3 Koordinierungsstelle für den Forschungsdatenzugang (KoForD)

(1) Es wird eine Koordinierungsstelle für den Forschungsdatenzugang eingerichtet.

(2) Die KoForD verfügt über ein Data-Governance Board (DaGoB) und ein Ethics Research Board (ERB).

(3) Die KoForD betreibt einen Hosting-Dienst nach höchsten IT-rechtlichen Standards, über den die Daten an den Antragsteller übermittelt oder über einen Arbeitsplatz-Zugriff zur Verfügung gestellt werden.

§ 4 Aufgaben der KoForD

(1) Die KoForD ist der Adressat von Forschungsdatenzugangsanträgen nach § 12 dieses Gesetzes.

(2) Sie koordiniert die Sammlung, Kombination und Vorverarbeitung von sowie die Zugangsgewährung zu in den Forschungsdaten-Hubs gespeicherten Gesundheitsdaten.

(3) [1]Geht ein berechtigter Datenzugangsantrag ein, trägt die KoForD die in den Forschungsdaten-Hubs gespeicherten Daten zusammen. [2]Sie stellt außerdem bei den nach § 8 dieses Gesetzes im Verzeichnis gelisteten privaten Initiativen einen Antrag auf Forschungsdatenzugangsgewährung zu den vom Antragsteller begehrten Daten. [3]Die zusammengestellten Daten stellt sie dem Antragsteller im Wege des Datenzugangs nach Maßgabe des § 5 Abs. 3 dieses Gesetzes zur Verfügung.

§ 5 Data Governance Board (DaGoB)

(1) [1]Das Data-Governance Board ist ein unabhängiges Entscheidungsgremium innerhalb der KoForD, das vom Bundesgesundheitsministerium ernannt wird und sich aus Vertretern von Wissenschaft und Praxis für den Umgang mit Gesundheitsdaten zusammensetzt. [2]Es besteht aus 8 Mitgliedern. [3]Es herrscht Geschlechterparität.

(2) [1]Das Data-Governance Board trifft die Entscheidung darüber, ob ein Forschungsdatenzugangsantrag berechtigt ist. [2]Das ist der Fall, wenn er den formalen und materiellen Voraussetzungen dieses Gesetzes entspricht und auch im Übrigen mit geltendem Recht vereinbar ist.

(3) Das Data Governance Board entscheidet außerdem nach Prüfung des Schutzkonzeptes i.S.d. § 13 und in Anbetracht des daraus resultierenden Risikos für die Rechte und Interessen der vom Datenzugang betroffenen Personen darüber, ob die Daten in anonymisierter, pseudonymisierter oder unveränderter Art und Weise zugänglich gemacht werden, sowie darüber, ob sie dem Antragsteller

über den Hosting-Dienst übermittelt oder aber als Arbeitsplatz-Zugriff, der auch als reiner Lese-Zugriff ausgestaltet werden kann, bereitgestellt werden.

§ 6 Research Ethics Board (REB)

(1) [1]Das Research Ethics Board ist ein unabhängiges Entscheidungsgremium innerhalb der KoForD, das vom Bundesgesundheitsministerium ernannt wird und sich aus Vertretern von Wissenschaft und Praxis für den Umgang mit Gesundheitsdaten zusammensetzt. [2]Es besteht aus 8 Mitgliedern. [3]Es herrscht Geschlechterparität.

(2) [1]Das Research Ethics Board trifft die Entscheidung darüber, ob ein Forschungsdatenzugangsantrag den ethischen Anforderungen an wissenschaftliche Forschung entspricht. [2]Es gibt sich selbst Entscheidungsleitlinien, die im Einklang mit ethischen Standards stehen. [3]Die Leitlinien sind zu veröffentlichen.

§ 7 Forschungsdaten-Hubs

(1) [1]Es werden Forschungsdatenhubs eingerichtet, die jeweils Datensätze der Datenzubringer, allerdings jeweils begrenzt auf ein bestimmtes Krankheitsbild oder bestimmte Versichertendaten speichern. [2] Die Krebsregister der Länder und das Forschungsdatenzentrum am BfArM fungieren ebenfalls als Forschungsdaten-Hubs.

§ 8 Verzeichnis privater Gesundheitsdienstleistungen für den Datenzugang

(1) [1]Die KoForD führt ein Verzeichnis von Gesundheitsdienstleistern, die Gesundheitsdaten mit Einwilligung des Patienten zu Zwecken des Gesundheitsdatenzugangs speichern. [2]Auf die Möglichkeit des Broad Consent i.S.d. § 2 Nr. 5 wird hingewiesen. [3]Auf Antrag des jeweiligen Gesundheitsdienstleisters wird dieser Gesundheitsdienstleister in das Verzeichnis aufgenommen. [4]Im Falle eines berechtigten und ethisch vertretbaren Datenzugangsantrages fordert die KoForD die Gesundheitsdienstleister auf, Daten i.S.d. Datenzugangsantrags an die KoForD zu übermitteln. [5]Die KoForD speichert diese Daten lediglich zum Zwecke der Befriedigung des Datenzugangsantrags zwischen. [6]Die Daten sind nach Befriedigung des Datenzugangsantrags zu löschen.

(2) Nach Abs. 3 anerkannte Personal Information Management Systems (PIMS) können ebenfalls als Gesundheitsdienstleister in das Verzeichnis nach Abs. 1 eingetragen werden.

(3) PIMS, die

1. ein Sicherheitskonzept vorlegen, das eine Bewertung der Qualität und Zuverlässigkeit des Dienstes und der technischen Anwendungen ermöglicht und aus dem sich ergibt, dass der Dienst sowohl technisch als auch organisatorisch die rechtlichen Anforderungen an

den Datenschutz und die Datensicherheit, die sich insb. aus der Verordnung (EU) 2016/679 ergeben, erfüllt und

2. die übermittelten Daten für keine anderen Zwecke als den durch die Datengeber definierten Zwecken verarbeiten

sind anzuerkennen.

(4) Die Bundesregierung bestimmt durch Rechtsverordnung mit Zustimmung des Bundestages und des Bundesrates die Anforderungen an das Verfahren der Anerkennung, insb.

1. den erforderlichen Inhalt des Antrags auf Anerkennung,
2. das Verfahren der Anerkennung,
3. den Inhalt des Sicherheitskonzepts nach Abs. 2 Nummer 1 und
4. die für die Anerkennung zuständige unabhängige Stelle.

(5) Anerkannte PIMS agieren als Stellvertreter der Datengeber und übermitteln personenbezogene Daten auf Grundlage einer dynamischen Einwilligung.
(6) Auf Aufforderung des Betroffenen sind die bei den Gesundheitsdienstleistern gespeicherten Daten auch ohne Anforderung durch die KoForD in die Forschungsdaten-Hubs zu übermitteln und dort zu speichern (Datenspende).
(7) Es sind geeignete Schnittstellen und Standards für die Datenübermittlung nach Abs. 1, 2 und 4 zur Verfügung zu stellen, die von der Bundesregierung durch Rechtsverordnung mit Zustimmung des Bundestages und des Bundesrates bestimmt werden.

§ 9 Übermittlung von Daten in die Forschungsdaten-Hubs
(1) [1]Datenzubringer, die nicht unter § 8 fallen, sind verpflichtet, diejenigen Daten in den Forschungsdaten-Hubs zu speichern, für die Forschungsdaten-Hubs eingerichtet werden. [2]Die Einrichtung eines Forschungsdaten-Hubs wird von der Bundesregierung durch Rechtsverordnung mit Zustimmung des Bundestages und des Bundesrates bestimmt.
(2) [1]Die übermittelten Daten werden von dem Forschungsdaten-Hub unmittelbar nach ihrem Eingang pseudonymisiert, verschlüsselt und mit einer Arbeitsnummer versehen. [2]Der Schlüssel und das Lieferpseudonym nebst Arbeitsnummer werden ausschließlich bei der Vertrauensstelle nach § 303c SGB V hinterlegt und bei dem Forschungsdaten-Hub gelöscht.

(3) Es sind geeignete Schnittstellen und Standards für die Datenübermittlung nach Abs. 1 zur Verfügung zu stellen, die von der Bundesregierung durch Rechtsverordnung mit Zustimmung des Bundestages und des Bundesrates bestimmt werden.
(4) [1]Patienten haben jederzeit das Recht, ohne Angabe von Gründen Auskunft darüber zu verlangen ob und ggf. welche Daten von Ihnen in den Forschungsdaten-Hubs gespeichert sind. [2]Für das Auskunftsverlangen sind die Vorschriften von DSGVO und BDSG maßgeblich.
(5) [1]Patienten haben jederzeit das Recht, ohne Angabe von Gründen die Löschung der sie betreffenden personenbezogenen Daten aus den Forschungsdaten-Hubs zu verlangen. [2]Die zu löschenden Daten sind hinreichend präzise zu bezeichnen. Dem Löschungsverlangen ist binnen Monatsfrist zu entsprechen.

§ 10 Datenzugang von Wissenschaft und Forschung
(1) Forschung und Wissenschaft haben zu Zwecken der Forschung im Gemeinwohlinteresse einen Anspruch auf Zugang zu den in den Forschungsdaten-Hubs sowie bei den Gesundheitsdienstleistern gespeicherten personenbezogenen Daten, sofern die Voraussetzungen der §§ 12, 13 und 15 erfüllt sind.
(2) [1]Im Gemeinwohlinteresse liegt eine Tätigkeit, deren Erbringung nicht allein durch individuelle – wirtschaftliche, eigennützige, freundschaftliche oder familiäre – Ziele motiviert ist, sondern sich zumindest auch als Ausdruck gesellschaftlicher Verantwortung erweist. [2]Das Gemeinwohlinteresse wird widerleglich vermutet, sofern der Antragsteller an einer Hochschule, einer nach landesrechtlichen Vorschriften anerkannten Hochschulklinik, oder einer öffentlich geförderten außeruniversitären Forschungseinrichtung tätig ist.
(3) Versicherungen und ihre Mitarbeiter sowie Personen, die im Auftrag oder im Interesse von Versicherungen tätig sind, sind nicht antragsberechtigt.
(4) Wird Zugang zu den bei Gesundheitsdienstleistern gespeicherten personenbezogenen Daten begehrt, so besteht der Anspruch nur, wenn der Betroffene seine Einwilligung für den Forschungsdatenzugang erklärt und nicht widerrufen hat.
(5) [1]Der Datenzugangsantrag ist einer Prüfung durch das DaGoB zuzuführen, das nach Maßgabe von § 5 Abs. 3 über die konkrete Art des Datenzugangs entscheidet. [2]Die Entscheidung über den Datenzugangsantrag kann mit Auflagen und Bedingungen versehen werden.
(6) Der Datenzugangsantrag ist einer Entscheidung über die ethische Vereinbarkeit durch das REB zuzuführen.
(7) [1]Eine positive Bescheidung des Datenzugangsantrags kann jederzeit widerrufen werden, wenn sich herausstellt, dass gegen die Vorgaben dieses Gesetzes verstoßen wird. [2]Er ist zu widerrufen, wenn sich

nachträglich herausstellt, dass die Voraussetzungen der Gewährung des Datenzugangs zum Zeitpunkt der Datenzugangsentscheidung nicht vorlagen.

§ 11 Anonymisierung und Pseudonymisierung der zugangsbetroffenen Daten

(1) Für die Anonymisierung und Pseudonymisierung der Daten werden Standards entwickelt.

(2) Zur Entwicklung dieser Standards wird ein Expertenrat bestehend aus Vertretern aus Wissenschaft und Praxis eingesetzt.

(3) Bei Einhaltung der Standards wird widerleglich vermutet, dass eine Anonymisierung bzw. Pseudonymisierung erfolgt ist.

(4) Die De-Anonymisierung von nach Abs. 1 anonymisierten Daten wird mit Freiheitsstrafe von bis zu einem Jahr oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

§ 12 Antragsvoraussetzungen

Der Antrag ist über das elektronische Antragsportal zu stellen.

§ 13 Schutzkonzept

(1) Der Datenzugang darf nur erfolgen, wenn der Antragsteller der KoForD ein Schutzkonzept vorlegt.

(2) Das Schutzkonzept beinhaltet

1. eine Beschreibung der für die Forschungszwecke erforderlichen Daten,
2. eine Beschreibung der beabsichtigten Verwendung der Daten
3. eine Beschreibung der Vorkehrungen, um eine anderweitige Verwendung der Daten zu verhindern,
4. eine Beschreibung der Vorkehrungen, um die schutzwürdigen Interessen des Anbieters zu schützen und
5. eine Beschreibung der technischen und organisatorischen Maßnahmen, die den Schutz der personenbezogenen Daten sicherstellen.

(3) Das Schutzkonzept ist zugleich mit dem Auskunftsverlangen an die zuständige Datenschutzaufsichtsbehörde zu übermitteln.

§ 14 Frist der Datenzugangsgewährung

[1]Die Entscheidung über den Datenzugang ist spätestens drei Monate nach Eingang des vollständigen Antrags bei der Behörde zu treffen. [2]Das DaGoB kann die Bearbeitungszeit um maximal 3 Monate verlängern, wenn die Bearbeitung des Antrags und des zugehörigen Schutzkonzeptes eine ungewöhnlich umfangreiche Verarbeitung von Daten oder einen besonders anspruchsvollen Abwägungsprozess erfordert. [3]KoForD muss den Antragsteller über die Fristverlängerung, die

Begründung für die Verlängerung und die neue Frist, bis zu der die Entscheidung über die Genehmigung ergeht, informieren.

§ 15 Schranken

Der Datenzugang darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

§ 16 Gebühren

[1]Für die Gewährung des Forschungsdatenzugangs kann eine Gebühr erhoben werden. [2]Es gelten die Vorschriften der Datentransparenz-Gebührenverordnung.

§ 17 Nachnutzung

(1) [1]Die Forschungsergebnisse sind in nach Maßgabe des § 11 anonymisierter Form zu veröffentlichen. [2]Die Fundstelle der Veröffentlichung ist auf der Webpräsenz der KoForD anzugeben.

(2) Die vom Datenzugang betroffenen Daten sind nach Abschluss des Forschungsprojektes beim Datenzugangsberechtigten zu löschen, spätestens aber, sobald eine Speicherung der Daten nicht mehr erforderlich ist.

(3) Die vom Datenzugang betroffenen Daten dürfen nicht an Dritte weitergegeben werden.

(4) [1]Ein Verstoß gegen die Abs. 1-3 führt zu einem Ausschluss von der Antragsberechtigung von 3 Jahren. [2]In besonders schweren Fällen kann das DaGoB einen längeren Ausschluss anordnen.

§ 18 Datentreuhandsysteme

(1) Zum Zwecke der Aggregation und Auswertung von Datenbeständen durch Wissenschaft und Forschung im Gemeininteresse dürfen Daten auch ohne die Einwilligung des Betroffenen an anerkannte Datentreuhandsysteme übermittelt und dort i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet werden.

(2) Datentreuhandsysteme, die

1. ein Sicherheitskonzept vorlegen, das eine Bewertung der Qualität und Zuverlässigkeit des Dienstes und der technischen Anwendungen ermöglicht und aus dem sich ergibt, dass der Dienst sowohl technisch als auch organisatorisch die rechtlichen Anforderungen an den Datenschutz und die Datensicherheit, die sich insb. aus der Verordnung (EU) 2016/679 ergeben, erfüllt und

2. die übermittelten Daten für keine anderen Zwecke als den durch die Datengeber definierten Zwecken verarbeiten

sind anzuerkennen.

(3) Die Bundesregierung bestimmt durch Rechtsverordnung mit Zustimmung des Bundestages und des Bundesrates die Anforderungen an das Verfahren der Anerkennung, insb.

1. den erforderlichen Inhalt des Antrags auf Anerkennung,
2. den Inhalt des Sicherheitskonzepts nach Abs. 2 Nummer 1
3. das Verfahren der Anerkennung und
4. die für die Anerkennung zuständige unabhängige Stelle.

(4) [1]Die Daten sind nach der Verarbeitung aus der Datentreuhand zu löschen. Eine Weitergabe ist untersagt. [2]§ 42 BDSG findet Anwendung.

Aufgrund der Regelung des § 12 Abs. 2 TMG ist – weil auch Diensteanbieter i.S.d. TMG von dem GFDZG betroffen sind – außerdem im TMG die Befugnis zur Übermittlung von Daten zur Erfüllung von Datenzugangsansprüchen vorzusehen. Es bietet sich an, dies in § 14 Abs. 6 TMG zu normieren.

2. Online-Wirtschaftssektor

Im Online-Wirtschaftssektor finden sich allein im nationalen Recht Forschungsklauseln. Diese sind sämtlich erst kürzlich eingeführt worden oder liegen, wie im Falle des DSA, bislang erst als Entwurfsfassung vor, weshalb für die Analyse weder auf Rechtsprechung noch auf Kommentarliteratur zurückgegriffen werden kann. Folgende Aspekte scheinen dennoch als geeignete Orientierungspunkte für die Normierung zukünftiger Forschungsdatenklauseln:

a) System abgeleiteter und originärer Forschungsklauseln normieren

Im Online-Wirtschaftssektor existieren bereits vereinzelt Datenzugangsansprüche Dritter, z.B. im GWB. Dort, wo Dritte Zugang zu Daten erhalten, empfiehlt sich eine Prüfung der Gleichwertigkeit der anerkannten Zugangsinteressen Dritter und denen der Forschung. Bejahendenfalls sollten an die existenten Datenzugangsansprüche zugunsten von Wissenschaft und Forschung als abgeleitete Datenzugangsansprüche angelehnt werden. Diese können entweder unmittelbar in dem Gesetz geregelt werden, das den originären Datenzugangsanspruch der Dritten vorsieht, oder aber im Rahmen eines allgemeinen Forschungsdatenzugangsgesetzes, wobei eine Normierung unmittelbar in dem Gesetz, das den originären Datenzugangsanspruch der Dritten vorsieht aufgrund der Sachnähe der Regelung vorzuziehen ist, auch wenn der Sinn und Zweck des Gesetzes möglicherweise nicht auf den Forschungsdatenzugang gerichtet ist.

b) Zugang zu den Daten privater und öffentlicher Stellen durch mittelbare Datenzugangsstrukturen in staatlicher Organisation ermöglichen

Im Online-Wirtschaftssektor sind Forschungsdatenzugangsansprüche in der Regel gegen private Stelle gerichtet. Sowohl § 19 Abs. 3 UrhDaG als auch in § 5a NetzDG sind als unmittelbare Ansprüche gegen private Stellen vorgesehen. Dies dürfte in der Praxis zu nicht unerheblichem Aufwand und Kosten durch die Prüfung der Datenzugangsansprüche führen. Auf die Betroffenen dürfte vielfach dasselbe Haftungsdilemma zukommen wie wir es in Fällen der Urheberrechtsverletzung oder auch der Markenrechts- und Persönlichkeitsrechtsverletzungen im Netz vorfinden: Die Anspruchsverpflichteten sind einerseits für eine fehlerhafte Versagung des Datenzugangs haftbar, andererseits aber ebenso für eine zu Unrecht erfolgende Datenzugangsgewährung. Dieses Haftungsdilemma führt schon im Urheber-, Marken- und Persönlichkeitsrecht zu einer für alle Beteiligten als unbefriedigend wahrgenommenen Situationen, die für die Forschungsdatenzugangsansprüche nicht zum Vorbild genommen werden sollten. Art. 33 DSA-E geht hingegen einen anderen Weg: Er erklärt den Koordinator für digitale Dienste zum Entscheidungsträger über die Datenzugangsgewährleistung. Auf sein Verlangen hin muss den anspruchsberechtigten Forschern Datenzugang gewährt werden. Im

Unterschied zum Gesundheitssektor werden die Daten, zu denen Zugang gewährt werden soll, nicht zentral in Research Data Hubs vorgehalten, sondern bleiben dezentral bei den Anspruchsverpflichteten gespeichert. Der Koordinator für digitale Dienste übernimmt lediglich die Datenzugangsentscheidung. Eine solche mittelbare Datenzugangsgewährungsinfrastruktur im Online-Wirtschaftssektor scheint sinnvoll, um Aufwand und Kosten der Anspruchsverpflichteten auf ein verhältnismäßiges Maß zu begrenzen.

c) Datenzugangsanspruch nicht generell auf spezifische Forschungsvorhaben beschränken

Die de lege lata existenten Datenzugangsansprüche sind sämtlich beschränkt auf Daten, die für spezifische Forschungsvorhaben benötigt werden, z.B. auf Daten über den Einsatz von Verfahren zur automatisierten Erkennung und Blockierung von Inhalten, § 19a Abs. 3 UrhDaG, oder Daten zur Ermittlung und zum Verständnis systemischer Risiken, Art. 31 DSA-E. Das greift aber zu kurz. Sämtliche Forschungsvorhaben, für die Datenzugang gewährleistet werden muss, gesetzlich präzise zu definieren, würde eine effektive Forschung im Gemeinwohlinteresse über Jahre hinter den tatsächlichen Entwicklungen hinterherhinken lassen. Außerdem droht eine unüberschaubare Anzahl möglicher Datenzugangsklauseln. Vielmehr sollte auch hier der Forschungsdatenzugang an das Gemeinwohlinteresse gebunden werden, über dessen Erfüllung ein beim Koordinator für Digitale Dienste anzusiedelndes Data Governance Board entscheidet. Die dem Datenzugangsanspruch unterliegenden Daten sollten darüber hinaus auf diejenigen Daten beschränkt werden, die der Anspruchsverpflichtete ohnehin erhoben hat und er sollte anders als im Gesundheitssektor auf die zweckbedingt erforderlichen Daten beschränkt werden. Eine Pflicht zur Erhebung von Daten durch den Zugangsverpflichteten begründet der Datenzugangsanspruch nicht. Eine weitere Beschränkung auf nur spezifische Daten, wie es heute vorherrschend ist, muss nicht stattfinden. Wird eine Beschränkung auf spezifische Daten nicht vorgenommen, sollten die zugangsverpflichteten Unternehmen aber in Anbetracht unterschiedlicher Leistungsfähigkeit bei der Gewährleistung von Datenzugang eine gewisse Größe aufweisen müssen. Kleinere Unternehmen würden anderenfalls durch die Pflicht zur Datenzugangsgewährung wirtschaftlich auch dann überfordert, wenn sie für die Gewährung des Datenzugangs vergütet würden. Ab welcher Größe Unternehmen zum Datenzugang verpflichtet werden können, sollte durch entsprechende Studien untersucht werden.

d) Datenzugangsvoraussetzungen am Gesundheitssektor orientieren

aa) Anspruchsberechtigung weit fassen

Insb. in der Anspruchsberechtigung sollte sich für den Online-Wirtschaftssektor am Gesundheitssektor orientiert werden. Die Fassung der Anspruchsberechtigung in § 19a Abs. 3 UrhDaG ist zu eng, weil sie kommerzielle Forschung zu weitreichend begrenzt. Artikel 31 DSA-E fordert sogar eine Zulassung der

Forscher. Dies alles trägt dazu bei, den Forschungsdatenzugangsanspruch unattraktiv auszugestalten und ihm damit seine Effektivität zu nehmen. Wie für den Gesundheitssektor dargelegt, sollte es nicht darauf ankommen, wer Forschung betreibt, sondern zu welchem Zweck die Forschung betrieben wird. Im Sinne des Five Safes Models sollte ein effektiver Schutz der betroffenen Rechte und Interessen von Anspruchsverpflichteten und Drittbetroffenen dann über die weiteren Anspruchsvoraussetzungen sichergestellt werden. In der Struktur als Orientierungspunkt dienen kann § 5a NetzDG, der die Anspruchsberechtigung zunächst weit auf Forscher (definiert als natürliche oder juristische Person, die wissenschaftliche Forschung betreibt) insgesamt bezieht und in § 5a Abs. 3 den Charakter der Forschung sodann auf Vorhaben im öffentlichen Interesse beschränkt. Das öffentliche Interesse sollte hier dem Begriff des Gemeinwohlinteresses weichen. Es sollte – wie auch im Gesundheitssektor – vermutet werden, wenn die Forschung an öffentlichen Forschungseinrichtungen im o.g. Sinne erbracht und die Forschungsergebnisse in anonymisierter Form der Öffentlichkeit zugänglich gemacht werden. Die Zugänglichmachung der Forschungsergebnisse sollte auch für die private Forschung als obligatorische Voraussetzung zur Bestimmung des Gemeinwohlinteresses der Forschung dienen, die aber freilich lediglich notwendige nicht aber hinreichende Voraussetzung sein kann.

bb) Zusätzliche Voraussetzungen von Datenzugang und Datenzugangsantrag vorsehen, Regelung der Anschlussnutzung definieren

Auch im Online-Wirtschaftssektor scheint die Einbindung von REB und DaGoB sinnvoll, um unterschiedliche Entscheidungen durch unterschiedliche Kompetenzträger treffen zu können. Auch sollte ein Schutzkonzept vorgelegt werden müssen, anhand dessen die Risiken für die konfligierenden Rechte und Interessen beurteilt werden können. Auch hier ist § 5a NetzDG wegweisend. Die Einreichung des Datenzugangsantrags beim Koordinator für Digitale Dienste sollte über ein standardisiertes Antragsformular sowie über standardisierte Übermittlungswege erfolgen können. Auch die Regelung der Anschlussnutzung sollte dem Gesundheitssektor entsprechend ausgestaltet sein.

e) Schrankenbestimmungen vorsehen

Auch im Online-Wirtschaftssektor kann der Datenzugangsanspruch nicht unbeschränkt vorgesehen werden. Anders als im Gesundheitssektor spielen hier aber nicht nur die grundrechtlich verbürgten Rechte der Betroffenen (insb. das Informationelle Selbstbestimmungsrecht) eine Rolle, sondern auch und gerade die grundrechtlich verbürgten Rechte der Anspruchsverpflichteten. Dies sind insb. Geistige Eigentumsrechte und der Geschäftsgeheimnisschutz. Um diese angemessen zu schützen, ist neben den rechtlichen und technischen Gewährleistungen, die auch im Gesundheitssektor erforderlich sind, eine Schrankenklausel notwendig. Diese ließe sich in Anlehnung an § 15 Abs. 4 DSGVO wie folgt fassen:

„Das Recht auf Datenzugang darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen."

Es entscheidet also im Falle kollidierender Rechte stets eine Grundrechtsabwägung über die Datenzugangsgewährung. Im Rahmen des Art. 15 DSGVO ist anerkannt, dass die hier normierte Auskunftspflicht in der Regel nicht gänzlich durch den Verweis auf überwiegende Rechte des Auskunftsverpflichteten oder Dritter versagt werden darf, sondern dass sie, sofern möglich, zumindest teilweise oder jedenfalls geschwärzt erfolgen muss.[328] Auch dies ließe sich aufgrund der gleichen Schutzrichtung von Datenzugangs- und Auskunftsanspruch auf den Datenzugangsanspruch übertragen.

f) Vergütungsregelungen und Frist der Datenzugangsverschaffung abweichend vom Gesundheitssektor regeln

Anders als im Gesundheitssektor sind im Online-Wirtschaftssektor die privaten Stellen im Falle eines berechtigten Datenzugangsanspruchs verpflichtet, die Daten bereit zu stellen. Dies kann mit einem erheblichen Aufwand verbunden sein, der zu entschädigen ist. Gleichzeitig kann eine überhöhte Vergütung die Effektivität des Datenzugangsanspruchs erheblich beeinträchtigen. § 5a NetzDG geht daher den Weg einer Höchstgrenze von 5.000 EUR und stellt die Angemessenheit der Höhe im Übrigen in das Ermessen des Gerichts nach § 287 ZPO. Dies scheint der einzig gangbare Weg, wobei die konkrete Bezifferung der Höchstgrenze je Anfrage zu bestimmen ist und bestenfalls evidenzbasiert festgelegt werden sollte.

Für die Frist der Datenzugangsgewährung muss auch hier gelten, dass diese abhängig vom Umfang des beantragten Datenzugangs sein muss, dennoch ist eine Höchstgrenze wünschenswert. Art. 31 DSA-E sieht hier vor, dass der Koordinator für digitale Dienste eine angemessene Frist setzt. Dies ließe sich um eine Höchstfrist von 3 Monaten in Anlehnung an den finnischen Secondary Use Act ergänzen, die nur in begründeten Ausnahmefällen einmalig verlängert werden kann.

g) Rechtsdurchsetzung und Beweislast mitdenken

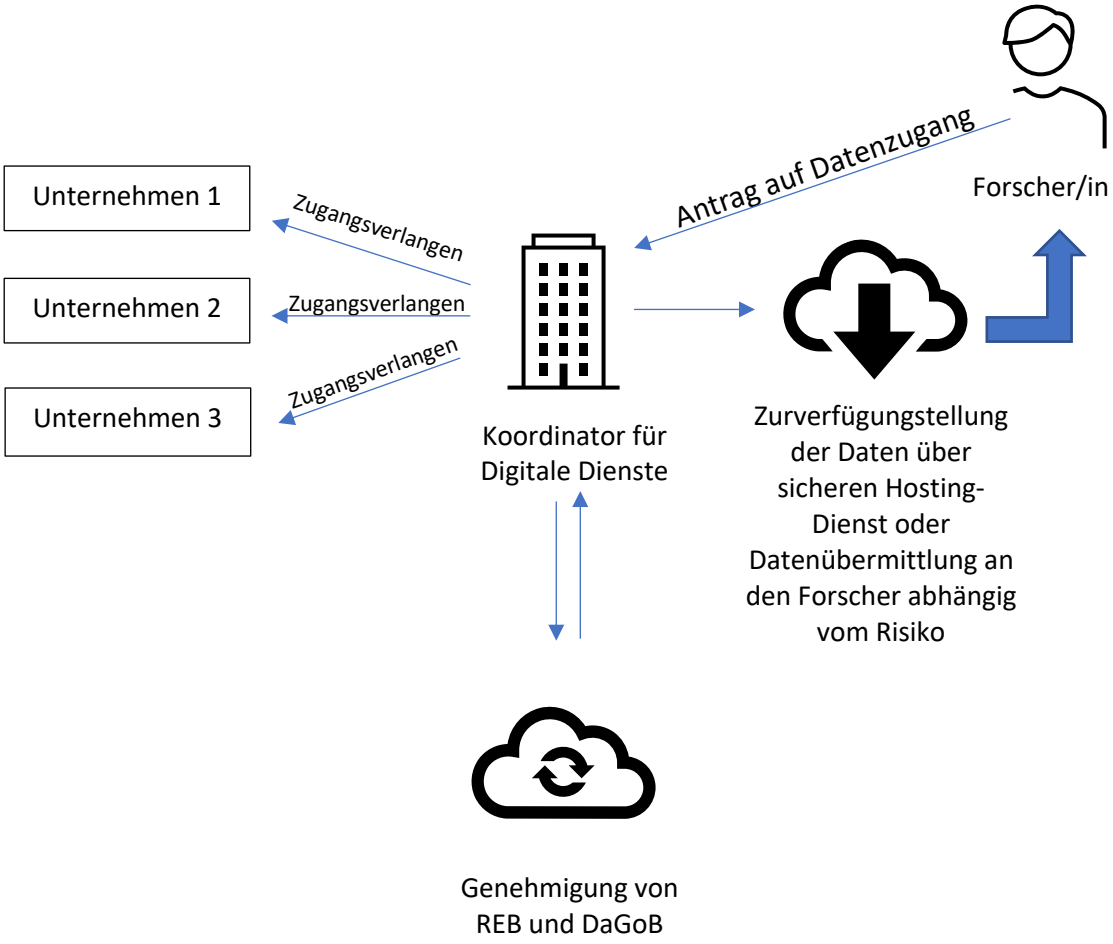
Gegen die Entscheidung des Koordinators für digitale Dienste müssen sowohl die Forscher als auch die Zugangsverpflichteten vorgehen können. Für den Fall der Versagung der Datenzugangsgewährung von Seiten des Zugangsverpflichteten sollte der Anspruchsberechtigte den Anspruchsverpflichteten in Anspruch nehmen können, ohne ein weiteres Tätigwerden des Koordinators für digitale Dienste abwarten zu müssen. Versagt der Koordinator für digitale Dienste dem Anspruchsberechtigten den Anspruch, so kann der Anspruchsberechtigte im Wege der Verpflichtungsklage gegen diesen vorgehen.

[328] *Specht*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Auflage, 2018, Art. 15 Rn. 16.

h) Empfohlenes Datenzugangsökosystem im Online-Wirtschaftssektor

Das für den Online-Wirtschaftssektor empfohlene Datenzugangsökosystem lässt sich wie folgt visualisieren:

Abb. 17: Empfohlenes Datenzugangsökosystem für den Online-Wirtschaftssektor



i) Vorschlag einer Musterforschungsdatenzugangsklausel im Online-Wirtschaftssektor

Die Leitlinien für einen Datenzugangsanspruch lassen sich in eine Musterdatenzugangsklausel, die in verschiedenen Gesetzen (siehe dazu unter bb)) normiert werden sollte, fassen:

aa) Musterforschungsdatenzugangsklausel

(1) Auf Antrag von Forschung und Wissenschaft gegenüber dem Koordinator für Digitale Dienste gewährt [Bezeichnung des Zugangsadressaten] Datenzugang zu Zwecken der Forschung im Gemeinwohlinteresse in dem durch den Zweck erforderlichen Umfang, wenn die Voraussetzungen der

§§ 12, 13 und 15 GFDZG erfüllt sind und ein Data Governance Board und ein Research Ethics Board beim Koordinator für Digitale Dienste den Datenzugangsantrag bewilligt.

(2) Die Vorschriften der §§ 2, 5 und 6, des § 10 Abs. 2, 3, 5, 6 sowie der §§ 11, 13, 15, 17 GFDZG finden entsprechende Anwendung.

(3) Der Koordinator für Digitale Dienste setzt eine angemessene Frist von höchstens drei Monaten für die Datenzugangsgewährung, die nur auf begründetes Verlangen des Zugangsadressaten einmalig verlängert werden kann.

(4) Der Zugangsadressat hat gegenüber dem Antragsteller einen Anspruch auf Erstattung der durch die Datenzugangsgewährung entstehenden Kosten in angemessener Höhe, die durch den Koordinator für digitale Dienste festgelegt wird. Bei der Bestimmung der angemessenen Höhe ist zu berücksichtigen, dass die Kosten kein wesentliches Hindernis für die Geltendmachung des Datenzugangsanspruchs darstellen dürfen. § 287 Abs. 1 der Zivilprozessordnung ist entsprechend anzuwenden. Die erstattungsfähigen Kosten dürfen vorbehaltlich des Satzes 5 höchstens 5.000 EUR betragen. Dieser Betrag darf nur überschritten werden, wenn durch die Erteilung der Auskunft ein außergewöhnlich hoher Aufwand entsteht. Nach Vorlage des Schutzkonzepts nach § 13 GFDZG kann der Antragsteller vom Koordinator für Digitale Dienste einen unentgeltlichen Kostenanschlag innerhalb einer angemessenen Frist verlangen.

(5) Der Antrag ist über das elektronische Antragsportal des Koordinators für Digitale Dienste zu stellen.

(6) Geeignete Schnittstellen und Standards für die Datenübermittlung werden von der Bundesregierung durch Rechtsverordnung mit Zustimmung des Bundestages und des Bundesrates festgelegt.

(7) Versagt der [Bezeichnung des Zugangsadressaten] den Datenzugang, ist für Klagen des Antragsberechtigten gegen den [Bezeichnung des Zugangsadressaten] auf Gewährung des Datenzugangs der ordentliche Rechtsweg eröffnet. Versagt der Koordinator für Digitale Dienste die Antragstellung, so ist für Klagen des Antragsberechtigten gegen den Koordinator für Digitale Dienste der Verwaltungsrechtsweg eröffnet.

Aufgrund der Regelung des § 12 Abs. 2 TMG ist außerdem im TMG die Befugnis zur Übermittlung von Daten zur Erfüllung von Datenzugangsansprüchen vorzusehen. Es bietet sich an, dies in § 14 Abs. 6 TMG zu normieren.

bb) Identifikation geeigneter Gesetze zur Implementierung der Musterforschungsdatenzugangsklausel

Diese Musterforschungsklausel ließe sich im Sektor Online-Wirtschaft als abgeleitete Forschungsklausel anlehnen an:

- Art. 33a DSA
- § 20 Abs. 1a GWB
- § 19a GWB
- § 32e GWB
- Art. 17 DMA

Sie ließe sich als originäre Forschungsklausel verankern in:

- der KI-VO der EU-Kommission
- dem Data Act der EU-Kommission

Außerhalb der im Rahmen dieser Studie besprochenen Sektoren ließen sich Datenzugangsansprüche entsprechend der hier entwickelten Musterklausel auch in einem Großteil derjenigen Klauseln einfügen, die bislang nur eine Datenzugangsgewährungserlaubnis vorsehen. Dies sind insb.:

- § 476 StPO
- § 98 SGB XI
- § 119 SGB XII
- § 42a BZRG
- § 75 SGB X
- § 66 PStG
- § 14 Abs. 2 i.V.m. § 15 TPG
- § 24a Abs. 1 AZRG
- Landeskrankenhausgesetze
- § 35 Abs. 7 HMG
- § 88a Abs. 4 AufenthaltsG

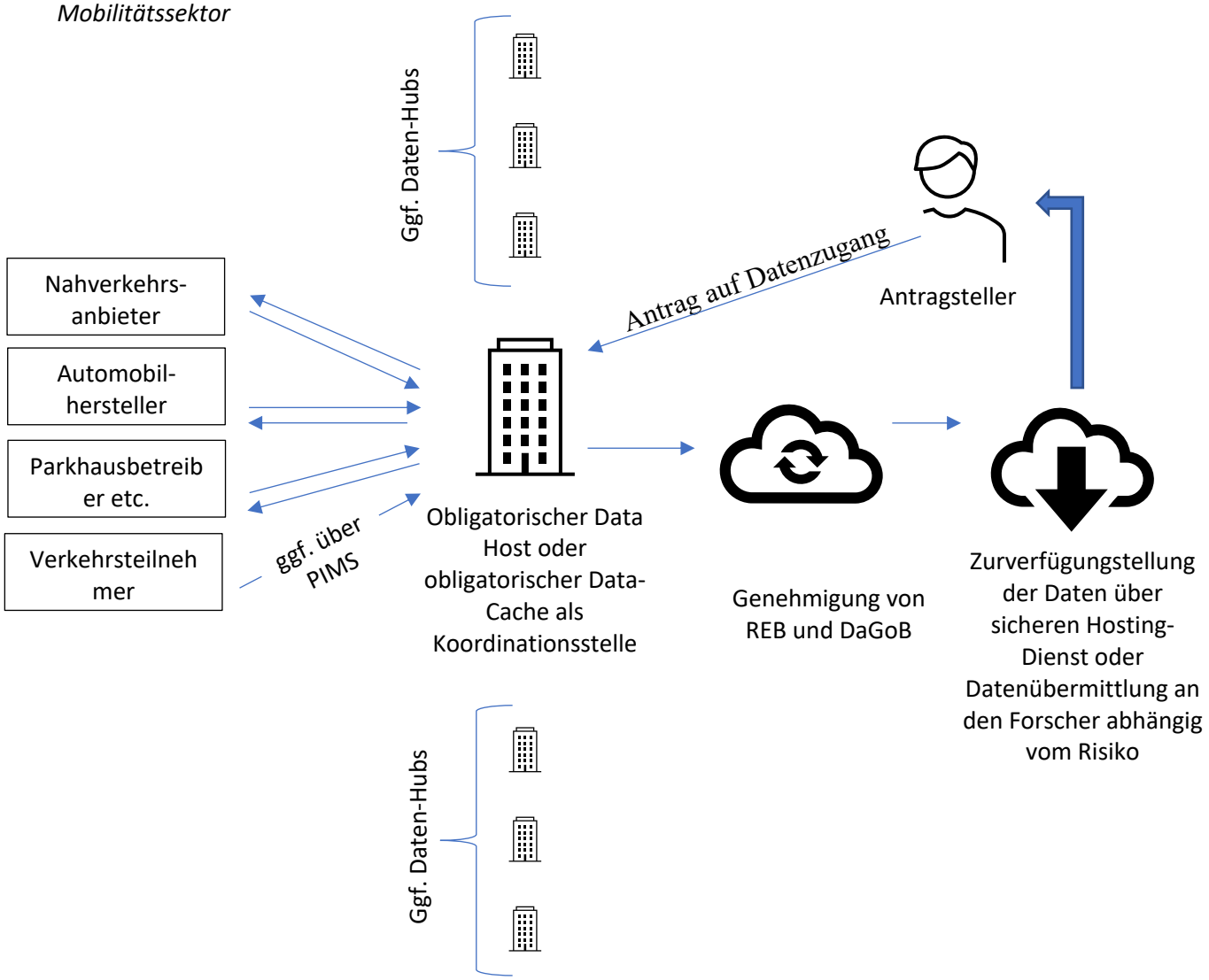
3. Mobilitätssektor

Im Mobilitätssektor sind die existenten Forschungsdatenzugangsansätze äußerst rudimentär. Weder in § 63a Abs. 5 StVG und § 1g Abs. 5 StVG lassen sich Orientierungspunkte ausmachen. Anspruchsberechtigung, erfasste Daten und Forschungszwecke scheinen vielmehr auch hier deutlich zu weit eingegrenzt. Da es sich aber ebenfalls um Datenzugangsansprüche gegen private Stellen handelt, ließen sich Teile aus dem Modell aus dem Online-Wirtschaftssektor übertragen. Insb. die Einrichtung einer Entscheidungsinstanz über den Datenzugang wird empfohlen. Fraglich ist aber, ob sich aus anderen Gründen, z.B. zur Eindämmung wettbewerblicher Probleme auf Sekundärmärkten, die Einrichtung eines obligatorischen Data Hosts statt eines obligatorischen Data Caches empfiehlt.[329] Daten, die heute allein im Automobil oder beim Fahrzeughersteller gespeichert werden, ließen sich dann (anonymisiert) zumindest auch im Data Host speichern (Shared-Server-Lösung) und entsprechend den gesetzlichen Vorgaben Dritten zugänglich machen. Aus datenschutzrechtlicher Perspektive empfiehlt sich dagegen eher eine dezentrale Speicherarchitektur. Vereinzelt existieren weitere Vorschläge von „Mobilitätsdatenplattformen“, die einen Austausch von Daten oder eine aggregierte Auswertung sowie ein föderales Lernen von Algorithmen über die aggregierten Daten ermöglichen sollen. Die Plattform Lernende Systeme schlägt etwa eine solche Mobilitätsdatenplattform zwecks föderalem Lernen vor, die beim Straßenbauamt oder aber beim TÜV angesiedelt sein könnte.[330] Das Projekt KI Data Tooling der VDA Leitinitiative könnte ebenfalls in eine Datentreuhandlösung zum Training von KI an aggregierten Datenbeständen münden. Dasselbe gilt für das von acatech getragene Projekt eines Mobilitätsdatenraumes, in dem Daten auf dem öffentlichen Nahverkehr, Parkhausauslastungen aber auch Daten Privater zusammengetragen werden, um ein verkehrsträgerübergreifendes und intermodales Mobilitätssystem in der Entstehung zu befördern.[331] Die Daten nach § 63a Abs. 1 StVG ließen sich ebenso in einer Datentreuhand speichern wie die nach § 1g Abs. 1 S. 2 StVG-E bereits heute durch das Kraftfahrtbundesamt als Datentreuhänder gespeicherten und von diesem nach und 1g Abs. 5 StVG an Forscher zu übermittelnden Daten. Die jeweiligen Plattformlösungen sollten unbedingt zusammengedacht werden. Es empfiehlt sich ein Koordinationsgremium aus Mitgliedern der Einzelprojekte sowie weiteren Experten, das die Projektideen in einem Mobilitätsdatenraum zusammenbringt und um die Komponente des Forschungsdatenzugangs erweitert. Auch Private Service-Anbieter wie z.B. Anbieter von Mobilitäts-Apps[332] könnten in das Datenzugangsökosystem entsprechend der Einbindung privater Service-

[329] So z.B. *Kerber*/*Gill*, Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, JIPITEC 2019, 244.
[330] *Hesse*/*Peylo* et al., Potenziale für ein industrieübergreifendes Flottenlernen, S. 20 ff.
[331] https://www.acatech.de/projekt/datenraum-mobilitaet/, zuletzt abgerufen am 16.07.2021.
[332] Die Open-Data Strategie der Bundesregierung v. 12.07.2021 weist beispielsweise auf Mobilitäts-Apps hin, die schon heute die Mobilitätsangebote zahlreicher Partner in einer einzigen App vereint, vgl. S. 11, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/open-data-strategie-der-bundesregierung.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 16.07.2021.

Anbieter im Gesundheitssystem eingebunden werden. Die Ausgestaltung allein eines Mobilitätsforschungsdatenzugangsgesetzes scheint aufgrund dieser komplexen Interessenlage mit Blick auf die Zugriffsbefugnisse nicht statthaft. Stattdessen sollte ein umfassender Mobilitätsdatenraum mit unterschiedlichen Zugriffsbefugnissen, z.B. von Wettbewerbern, Zulieferern, Reparatur- und Wartungsbetrieben, staatlichen Stellen aber auch datenschutzrechtlich Betroffenen und Forschern ausgestaltet werden. Ggf. ist zwischen unterschiedlichen Daten zu differenzieren, die möglicherweise in unterschiedlichen Data Hubs oder auch z.T. bei der datenerhebenden Stelle gespeichert werden könnten. Weder eine zentrale, noch eine dezentrale Datenspeicherung muss daher für sämtliche Daten und Problemlagen die statthafte Lösungsoption sein. Die Entwicklung eines solchen umfassenden Daten-Governance Modells und ihrer gesetzlichen Regelungen ist nicht Gegenstand dieses Gutachtens, ließe sich aber in Anlehnung an die hier ausgearbeiteten Ergebnisse wie folgt visualisieren, wobei insb. die betroffenen Daten, die Rolle der Speicherinstanz in Bezug auf verschiedene Daten, zwischen denen möglicherweise zu differenzieren ist, und der Kreis möglicher Antragsbefugter über Forschung und Lehre hinaus dringend weiter erörterungsbedürftig sind.

Abb. 18: Beispielhafte Veranschaulichung eines möglichen Datenzugangsökosystems im Mobilitätssektor



Der vom Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) eingerichtete Mobilitätsdatenmarktplatz („MDM-Plattform“) bringt ebenfalls Anbieter und Nutzer von Mobilitätsdaten zusammen und könnte in einer umfassenden Plattformlösung lediglich eine Auffangfunktion für vom Modell nicht erfasste Daten entfalten. Solange ein umfassendes Daten-Governance-Modell aussteht, kann und sollte Datenzugang für die Forschung im Mobilitätssektor aber jedenfalls durch eine abgeleitete Forschungsklausel in Anlehnung an Art. 6 Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typengenehmigung von Kraftfahrzeugen hinsichtlich der Emission von leichten Personenkraftwagen und Nutzfahrzeugen (EUR 5 und 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge[333] i.V.m. Art. 61 ff. der Verordnung 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern

[333] ABl. EU 2007 v. 29.06.2007, Nr. L 171/1.

sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG gewährt werden.

Die Regelungen zur Vergütung und zum Nachweis der Erfüllung der Verpflichtung der Zugangsgewährung sind bereits in den Art. 63 ff. der Verordnung 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge normiert und könnten auch für den Forschungsdatenzugang herangezogen werden.

Insofern wird folgende Formulierung des Art. 6 der Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typengenehmigung von Kraftfahrzeugen hinsichtlich der Emission von leichten Personenkraftwagen und Nutzfahrzeugen (EUR5 und 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge empfohlen:

Art. 6

(1)...

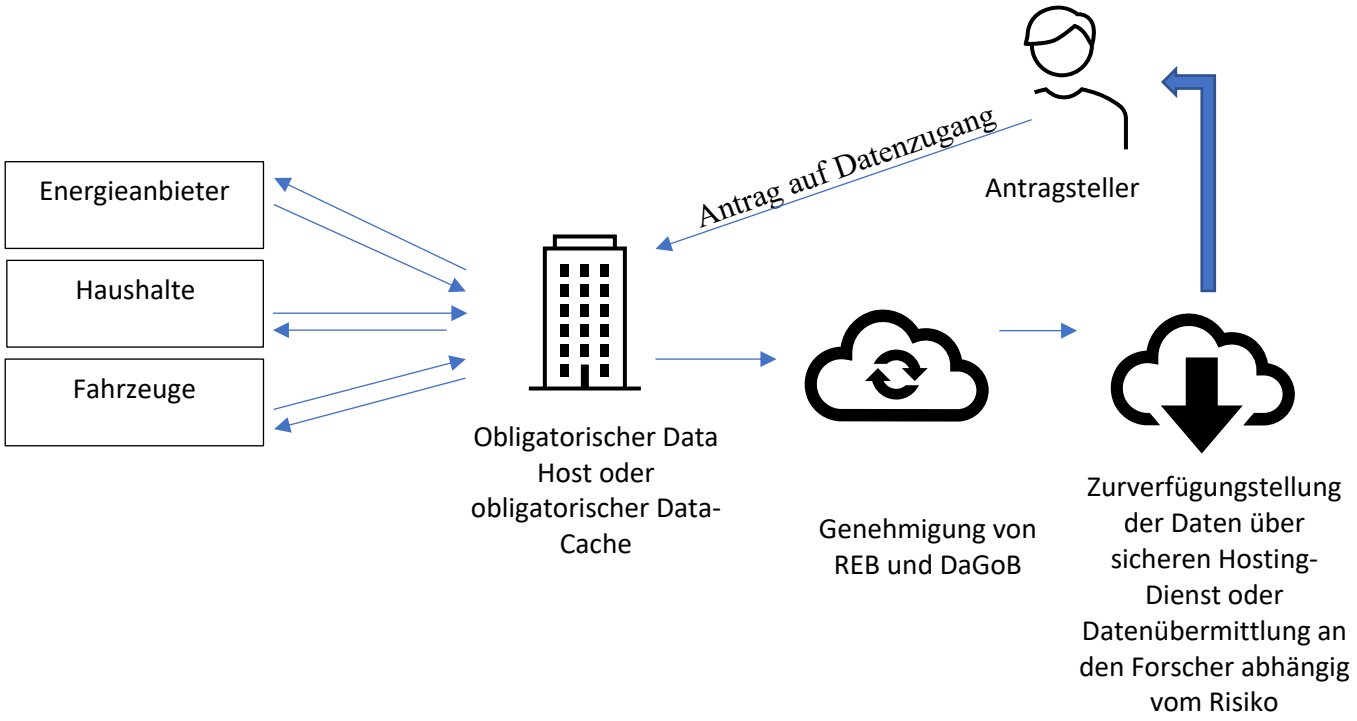
(2) Der Hersteller gewährt Datenzugang nach Abs. 1 auf Antrag von Personen aus Wissenschaft und Forschung auch zum Zwecke der Forschung im Gemeinwohlinteresse. Wissenschaft und Forschung umfasst jede Tätigkeit einer natürlichen Person oder einer Hochschule, einer nach landesrechtlichen Vorschriften anerkannten Hochschulklinik, einer öffentlich geförderten außeruniversitären Forschungseinrichtung oder einer sonstigen Einrichtung mit der Aufgabe wissenschaftlicher Forschung, mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen.
(3) Der Datenzugang ist innerhalb einer angemessenen Frist von höchstens drei Monaten zu gewähren, die nur auf begründetes Verlangen des Herstellers einmalig verlängert werden kann.

Darüber hinaus sollten § 1g Abs. 5 StVG und § 63a Abs. 5 StVG entsprechend der Musterforschungsdatenzugangsklausel im Online-Wirtschaftssektor ausgestaltet werden.

4. Energiesektor

Auch im Energiesektor existieren nur wenige Orientierungspunkte für die Ausgestaltung eines Forschungsdatenzugangs. Aus Großbritannien und Australien kann lediglich die Erkenntnis gewonnen werden, dass Datenzugang über einen zentralen Data-Host gewährleistet wird. Potentiell eingespeist werden könnten dort sämtliche Daten der Energieanbieter aber möglicherweise auch andere Energieverbrauchsdaten aus Haushalten, Fahrzeugen etc. Das Modell ließe sich sowohl mit einem obligatorischen Data Host als auch mit einem obligatorischen Data-Cache denken. In Ermangelung hinreichender Best-Practice Beispiele und Erfahrungen kann zu diesem Zeitpunkt weder ein Energieforschungsdatenzugangsgesetz, noch eine einzelne Musterforschungsklausel entwickelt werden. Vielmehr ist entsprechend dem Vorgehen in Großbritannien die Einrichtung einer Expertenkommission zu empfehlen, die ein Datenzugangsökosystem nebst konkreten Gesetzesvorschlägen für den Energiesektor erarbeitet, in dem Datenzugangsansprüche für die Forschung ebenfalls normiert sind. Insb. sollten die einzuspeisenden Daten identifiziert und erörtert werden, ob das Modell einer zentralen oder dezentralen Datenspeicherung, d.h. ein obligatorischer Data-Host oder ein obligatorischer Data Cache gewählt werden sollte oder eine Koordinationsstelle wie im Gesundheitssektor zu empfehlen ist. Auch über eine Erweiterung des Kreises der Antragsberechtigten ist nachzudenken. Im Übrigen kann sich an den für die übrigen Sektoren entwickelten Leitlinien orientiert werden, wodurch das Datenzugangsökosystem im Energiesektor zumindest für anonymisierte Daten wie unten abgebildet aussehen könnte. Für personenbezogene Daten empfiehlt sich eher ein System dezentraler Speicherung.

Abb. 19: Beispielhafte Veranschaulichung der Datenzugangsinfrastruktur im Energiesektor für anonymisierte Daten



XIII. Rechtspolitische Handlungsempfehlungen

Die Studienergebnisse lassen sich in 15 politische Handlungsempfehlungen fassen:

1. Die Maßstäbe eines Datenzugangs sollten sich insgesamt am „Five Safes Model“ orientieren, das Datenzugang in ein Spektrum von fünf Risikodimensionen einordnet, denen in der gesetzlichen Ausgestaltung des Datenzugangs zu begegnen ist.

2. Datenzugang sollte sich darüber hinaus an den FAIR-Prinzipien orientieren. Daten sollten auffindbar (findable), zugänglich (accessible), interoperabel (interoperable) und wiederverwendbar (reusable) sein.

3. Es empfiehlt sich die Ausgestaltung echter Forschungsklauseln im Sinne subjektiver Rechte auf Datenzugang für die Forschung in sämtlichen der hier untersuchten Sektoren, wobei die Empfehlungen je Sektor unterschiedlich weit reichen.

4. Im Gesundheitssektor sollte ein Gesamt-Forschungsdatenzugangsökosystem etabliert werden und in einem Gesundheitsforschungsdatenzugangsgesetz seinen Niederschlag finden. Es empfiehlt sich für den Gesundheitssektor die Verankerung originärer Forschungsklauseln sowie ein gemischtes System aus zentralen Datenspeichern (etwa bereits existenten Zentralregistern wie dem Bundeskrebsregister), dezentral-zentralen Datenspeichern (mehreren verteilten Registern mit gleichartigen Daten, wie den Landeskrebsregistern, wobei die Verteilung nicht zwingend nach Bundesländern erfolgen muss) und gänzlich dezentralen Datenspeichern z.B. bei Gesundheitsdiensteanbietern. In diesem System zentraler, dezentral-zantraler und gänzlich dezentraler Datenspeicher könnten - nach dem Vorbild v.a. Finnlands und Australiens aber auch Großbritanniens - sowohl bestimmte private als auch öffentlich gehaltene Daten nutzbar gemacht werden. Die Möglichkeit der Datenspende sollte auch und gerade über PIMS eröffnet werden.

5. Bei der regulatorischen Ausgestaltung von Datenzugangsansprüchen sollte in der Regel eine enge Zweckbindung an gemeinwohlorientierte Forschung normiert werden. Ist dies der Fall, muss der Kreis der Datenzugangsberechtigten nicht auf die nicht-kommerzielle Forschung beschränkt werden. Versicherungen sollten nach dem Vorbild Australiens von der Anspruchsberechtigung ausgeschlossen werden. Ein Erforderlichkeitskriterium des Datenzugangs ist nicht vorzusehen. Im Interesse des Schutzes konfligierender Rechte und Interessen sollte aber ein Schutzkonzept nach dem Vorbild des Netzwerkdurchsetzungsgesetzes Voraussetzung für den Datenzugang sein, und zwar unabhängig davon, ob die anonymisierte oder personenbezogene Daten vom Zugangsanspruch erfasst werden.

6. Für den Datenzugangsantrag sollte im Interesse einer effektiven Gewährleistung des Datenzugangs ein standardisiertes - idealerweise international einheitliches - Verfahren vorgesehen werden. Es empfiehlt sich außerdem die in einigen ausländischen Rechtsordnungen (Frankreich, Kanada, Finnland, Australien) vorgesehene Einbindung einer Instanz, die über die ethische Vereinbarkeit der Forschung entscheidet (Research Ethics Board) sowie einer Instanz, die über die materiell-rechtlichen Voraussetzungen und den Umfang der Datenzugangsgewährung entscheidet (Data Governance Board).

7. Die Anschlussnutzung der Daten sollte klar definiert werden. Sie sind frühestmöglich zu pseudonymisieren, zu anonymisieren oder zu löschen. Eine Nutzung der Daten zu kommerziellen Werbezwecken sollte ebenso untersagt werden, wie ein Verkauf der Daten. Auch eine gänzliche Untersagung der Datenweitergabe ist denkbar. Dies würde das Risiko einer missbräuchlichen Verwendung senken, weshalb der Datenzugangsanspruch zugunsten von Forschung und Wissenschaft im Gegenzug nach dem Five Safes Model weitreichender ausfallen dürfte als im Falle der Zulässigkeit einer Forschungsdatenweitergabe. Anonymisierte Daten sollten nicht de-anonymisiert werden dürfen, wobei das Verbot der De-Anonymisierung auch strafrechtlich adressiert werden sollte. Gleichzeitig sind im Interesse von Rechtsklarheit und zur Wahrung des Bestimmtheitsgebotes Standards zur Anonymisierung vorzusehen.

8. Der Datenzugang darf die Rechte und Interessen Dritter nicht über Gebühr einschränken. Dies ist als Schrankenbestimmung vorzusehen. Vergütungsregelungen sollten sich auf eine Kostendeckung der Verwaltungstätigkeit beschränken. Orientiert werden sollte sich an der Datentransparenz-Gebührenverordnung. Fristenregelungen im Verwaltungsbereich sollten stets einhergehen mit einer ausreichenden Personal- und Sachmitteldeckung. Gleichzeitig muss eine sorgfältige Prüfung des Datenzugangs gewährleistet sein. Flexible Fristenregelungen mit einer Obergrenze sind daher starren Fristenregelungen, die nicht oder nur unzureichend auf den konkreten Bearbeitungsaufwand reagieren können, vorzuziehen. Eine Orientierung an Finnlands Secondary Use Act ‚die Entscheidung über einen data-permit unverzüglich zu treffen, spätestens aber 3 Monate nach Eingang des vollständigen Antrags bei der Behörde, ist zu empfehlen.

9. Entscheidungen über den Datenzugang ergehen in dem hier entwickelten Gesundheitsdatenzugangsökosystem in der Form des Verwaltungsaktes. Der statthafte Rechtsweg für den Fall eines ablehnenden Bescheides ist daher die Verpflichtungsklage gerichtet auf den Erlass eines stattgebenden Verwaltungsaktes. Es gelten grundsätzlich die allgemeinen Beweislastregelungen. Das Gemeinwohlinteresse sollte aber, wenn die Forschung an öffentlichen Forschungseinrichtungen erbracht und die Forschungsergebnisse (anonymisiert) der Öffentlichkeit zugänglich gemacht werden, vermutet werden.

10. Neben einem System zentraler, dezentral-zentraler und gänzlich dezentraler Speicher von Forschungsdaten sollten flexible Datentreuhandstrukturen vorgesehen und auf eine rechtssichere Grundlage gestellt werden.

11. Für den Online-Wirtschaftssektor sollten Datenzugangsansprüche für Wissenschaft und Forschung entsprechend der hier vorgeschlagenen Musterforschungsdatenzugangsklausel in einer Reihe identifizierter Gesetze als abgeleitete und originäre Forschungsklauseln normiert werden. Eine abgeleitete Forschungsklausel sollte mindestens verankert werden in:

- Art. 33a DSA
- § 20 Abs. 1a GWB
- § 19a GWB
- § 32e GWB
- Art. 17 DMA

Eine originäre Forschungsklausel sollte insbesondere verankert werden in:

- der KI-VO der EU-Kommission
- dem Data Act der EU-Kommission

Außerhalb der im Rahmen dieser Studie besprochenen Sektoren ließen sich Datenzugangsansprüche entsprechend der hier entwickelten Musterklausel auch in einem Großteil derjenigen Klauseln einfügen, die bislang nur eine Datenzugangsgewährungserlaubnis vorsehen. Dies sind insb.:

- § 476 StPO
- § 98 SGB XI
- § 119 SGB XII
- § 42a BZRG
- § 75 SGB X
- § 66 PStG
- § 14 Abs. 2 i.V.m. § 15 TPG
- § 24a Abs. 1 AZRG
- Landeskrankenhausgesetze
- § 35 Abs. 7 HMG
- § 88a Abs. 4 AufenthaltsG

Vorschriften, bei denen bereits aus der Urteilsbegründung hervorgeht, dass es sich um Datenzugangsansprüche handeln soll, ohne dass dies im Gesetzestext eindeutig gefasst ist, lassen sich bereits durch Auslegung als subjektive Datenzugangsansprüche verstehen. Dies gilt etwa für § 1g StVG sowie für § 63a Abs. 5 StVG. Auch hier wäre aber zur Klarstellung eine Änderung des Wortlautes wünschenswert.

12. Auch im Online-Wirtschaftssektor sollte Zugang zu den Daten privater und öffentlicher Stellen durch mittelbare Datenzugangsstrukturen in staatlicher Organisation gewährleistet werden. D.h. konkret, dass entsprechend Art. 31 DSE-E der Koordinator für Digitale Dienste oder eine ähnliche Instanz über den Datenzugang entscheiden sollte, um die privaten Stellen von der Datenzugangsentscheidung zu entlasten.

13. Eine Beschränkung des Datenzugangsanspruchs auf spezifische Forschungsvorhaben muss nicht stattfinden. Wird eine solche Beschränkung nicht vorgenommen, empfiehlt sich aber eine asymmetrische Regulierung, d.h. eine Adressierung von Unternehmen der Privatwirtschaft erst ab einer gewissen Größe, die eine wirtschaftliche Überforderung durch die Verpflichtung zum Datenzugang ausschließt. Im Übrigen kann sich im Wesentlichen an den Datenzugangsvoraussetzungen im Gesundheitssektor orientiert werden. Anders als im Gesundheitssektor sind im Online-Wirtschaftssektor jedoch die privaten Stellen im Falle eines berechtigten Datenzugangsanspruches verpflichtet, die Daten bereit zu stellen. Dies kann mit einem erheblichen Aufwand verbunden sein, der zu entschädigen ist. Gleichzeitig kann eine überhöhte Vergütung die Effektivität des Datenzugangsanspruchs erheblich beeinträchtigen. Die konkrete Bezifferung der Datenzugangsvergütung sollte daher evidenzbasiert festgelegt werden und den Forschungsdatenzugangsanspruch nicht unangemessen hemmen.

14. Gegen die Entscheidung des Koordinators für digitale Dienste müssen sowohl die Forscher als auch die Zugangsverpflichteten vorgehen können. Für den Fall der Versagung der Datenzugangsgewährung von Seiten des Zugangsverpflichteten sollte der Anspruchsberechtigte den Anspruchsverpflichteten direkt in Anspruch nehmen können, ohne ein weiteres Tätigwerden des Koordinators für digitale Dienste abwarten zu müssen. Versagt der Koordinator für digitale Dienste dem Anspruchsberechtigten den Anspruch, so kann der Anspruchsberechtigte im Wege der Verpflichtungsklage gegen diesen vorgehen.

15. Im Mobilitätssektor und im Energiesektor sollte mangels nationaler und internationaler Best-Practice-Regelungen zunächst eine Expertenkommission eingesetzt werden, die Empfehlungen insb. für die von einem Datenzugangsanspruch erfassten Daten und die passende Datenzugangsinfrastruktur entwickelt. Im Mobilitätssektor sollten dabei die bereits von verschiedenen Stellen verfolgten Ansätze von Mobilitätsdatenräumen und -plattformen zusammen gedacht werden.

XIII. Literaturverzeichnis

Australian Government - Department of Health
Framework to guide the secondary use of My Health Record system data
Canberra 2018, S. 1-67
(zitiert als: Australian Government - Department of Health, Framework to guide the secondary use of My Health Record system data, 2018, S.)

Brink, Stefan;
Wolff, Heinrich Amadeus
Beck'scher Online-Kommentar Datenschutzrecht
36. Edition, München 2021
(zitiert als: Bearbeiter, in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, 2021, DS-GVO/BDSG § Rn.)

Buchholz, Wolf
Die neue PSI-Richtlinie - Wieviel Datenhoheit verbleibt den öffentlichen Unternehmen?
Infrastruktur Recht, Heft 8/2019, S. 197-200
(zitiert als: Buchholz, Die neue PSI-Richtlinie - Wieviel Datenhoheit verbleibt den öffentlichen Unternehmen?, IR 2019, Nennung Anfangsseite, Zitatseite)

Bundesministerium der Justiz und für Verbraucherschutz;
Max-Planck-Institut für Innovation und Wettbewerb
Data Access, Consumer Interests and Public Welfare
Berlin 2021, S. 1-574
(zitiert als: Bearbeiter, in: Bundesministerium der Justiz und für Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb, Data Access, Consumer Interests and Public Welfare, 2021, S.)

Bundesregierung
Open-Data Strategie der Bundesregierung
Berlin 2021, S. 1-32
(zitiert als: Bundesregierung, Die Open-Data Strategie der Bundesregierung v. 12.07.2021, S.)

Bundesregierung
Datenstrategie der Bundesregierung
Berlin 2021, S. 1-120
(zitiert als: Bundesregierung, Datenstrategie der Bundesregierung, 2021, S.)

Cuggia, Marc;
Polton, Dominique;
Wainrib, Gilles;
Combes, Stéphanie
Health Data Hub: Mission de Préfiguration
Paris 2018, S. 1-108.
(zitiert als: Cuggia/Polton/Wainrib/Combes, Health Data Hub: Mission de Préfiguration, 2018, S.)

Datenethikkommission
Gutachten der Datenethikkommission
Berlin 2019, S. 1-240
(zitiert als: Datenethikkommission, Gutachten der Datenethikkommission, 2018, S.)

Davenport, James Harold;
Grant, James;
Data Without Software Are Just Numbers
Data Science Journal, 19: 3, 2020, S. 1-6

Jones, Catherine Mary
(zitiert als: Davenport/Grant/Jones, Data Without Software Are Just Numbers, Data Science Journal 19 (3), 2020, S.)

Desai, Tanvi;
Ritchie, Felix;
Welpton, Richard
Five Safes: Designing data access for research
Economics Working Paper Series 1601, University of the West of England, Bristol 2016, S. 1-27
(zitiert als: Desai/Ritchie/Welpton, Five Safes: Designing data access for research, Economics Working Paper Series 1601, 2016, S.)

Deutsche Energie-Agentur
Schnittstellen und Standards für die Digitalisierung der Energiewende
Übersicht, Status Quo und Handlungsbedarf (dena-Analyse)
Berlin 2018, S. 1-58
(zitiert als: Deutsche Energie-Agentur, Schnittstellen und Standards für die Digitalisierung der Energiewende, 2018, S.)

Dierks, Christian
Rechtsgutachten Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern
Berlin 2019, S. 1-116
(zitiert als: Dierks, Rechtsgutachten Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, S.)

Dreier, Horst
Grundgesetz-Kommentar
2. Auflage, Tübingen 2004
(zitiert als: Bearbeiter, in: Dreier, Grundgesetz-Kommentar, 2. Auflage, 2004, Art. Rn.)

Ehlers, Dirk
Europäische Grundrechte und Grundfreiheiten
3. Auflage, Berlin 2009
(zitiert als: Bearbeiter, in: Ehlers, Europäische Grundrechte und Grundfreiheiten, 3. Auflage, 2009, § Rn.)

Epping, Volker;
Hillgruber, Christian
Beck'scher Online-Kommentar Grundgesetz
47. Edition, München 2015
(zitiert als: Bearbeiter, in: Epping/Hillgruber, BeckOK Grundgesetz, 47. Edition, 2021, Art. Rn.)

European Data Protection Supervisor
Opinion on Personal Information Management Systems
Opinion 9/2016, S. 1-20
(zitiert als: European Data Protection Supervisor, Opinion on Personal Information Management Systems, Opinion 9/2016, S.)

Feldmann, Thorsten
Zum Referentenentwurf eines NetzDG: Eine kritische Betrachtung
Kommunikation & Recht, Heft 5/2017, S. 292-297
(zitiert als: Feldmann, Zum Referentenentwurf eines NetzDG: Eine kritische Betrachtung, K&R 2017, Nennung Anfangsseite, Zitatseite)

Franzius, Claudio
Das Recht auf informationelle Selbstbestimmung
Zeitschrift für das Juristische Studium, Heft 3/2015, S. 259-270
(zitiert als: Das Recht auf informationelle Selbstbestimmung, ZJS 2015, Nennung Anfangsseite, Zitatseite)

Fraunhofer-Institut für Verkehrs- und Infrastruktursysteme IVI
Mobility Data Spaces
Dresden 2020, S. 1-21
(zitiert als: Fraunhofer-Institut für Verkehrs- und Infrastruktursysteme IVI, Mobility Data Spaces, 2020, S.)

Geiger, Christophe
Research Handbook on Human Rights and Intellectual Property
Cheltenham 2016, S. 1-752
(zitiert als Bearbeiter, Titel, in: Geiger, Research Handbook on Human Rights and Intellectual Property, 2016, S.)

Gierschmann, Sybille; Schlender, Katharina; Stentzel, Rainer; Veil, Winfried
Kommentar Datenschutz-Grundverordnung
Berlin 2017
(zitiert als: Bearbeiter, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar DSGVO, 2017, Art. Rn.)

Gola, Peter
Datenschutz-Grundverordnung: DS-GVO
2. Auflage, München 2018
(zitiert als: Bearbeiter, in: Gola, Datenschutz-Grundverordnung, 2. Auflage, 2018, Art. Rn.)

Government of India, Ministry of Electronics and Information Technology, Committee of Experts on Non-Personal Data Governance Framework
Report by the Commitee of Experts on Non-Personal Data Governance Framework
Dezember 2020, S. 1-62
(zitiert als: Report by the Commitee of Experts on Non-Personal Data Governance Framework, Dezember 2020, S.)

Graf von Kielmannsegg, Sebastian
Gesetzgebung im Windschatten der Pandemie: § 287a SGB V und der Datenschutz in der Gesundheitsforschung
Verwaltungsarchiv, 112/2021, S. 133-168
(zitiert als: von Kielmannsegg, Gesetzgebung im Windschatten der Pandemie: § 287a SGB V und der Datenschutz in der Gesundheitsforschung, VerwArch 2021, Nennung Anfangsseite, Zitatseite)

Graf, Jürgen
Beck'scher Online-Kommentar StPO
39. Edition, München 2021
(zitiert als: Bearbeiter, in: Graf, BeckOK StPO, 39. Edition, 2021, § Rn.)

Grünwald, Andreas;
Nüßing, Christoph
Vom NetzDG zum DSA: Wachablösung beim Kampf gegen Hate Speech?
Multimedia und Recht, Heft 4/2021, S. 283-287
(zitiert als: Grünwald/Nüßing, Vom NetzDG zum DSA: Wachablösung beim Kampf gegen Hate Speech?, MMR 2021, Nennung Anfangsseite, Zitatseite)

Hain, Karl-E.;
Ferreau, Frederik;
Brings-Wiesen, Tobias
Regulierung sozialer Netzwerke revisited
Kommunikation & Recht, Heft 7/2017, S. 433-438
(zitiert als: Hain/Ferreau/Brings-Wiesen, Regulierung sozialer Netzwerke revisited, K&R 2017, Nennung Anfangsseite, Zitatseite)

Härting, Niko;
Tekin, David
Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG-E)
IP-Rechtsberater, Heft 3/2020, S. 69-72
(zitiert als: Härting/Tekin, Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG-E), IPRB 2020, Nennung Anfangsseite, Zitatseite)

Heidhues, Paul;
Köster, Mats;
Köszegi, Botond
Steering Fallible Consumers
2021, S. 1-48
(zitiert als: Heidhues/Köster/Köszegi, Steering Fallible Consumers, S.)

Hesse, Tobias;
***Peylo, Christoph* et al.**
Potenziale für ein industrieübergreifendes Flottenlernen – KI-Mobilitätsdatenplattform zur Risikominimierung des automatisierten Fahrens. Whitepaper aus der Plattform Lernende Systeme
München 2021, S. 1-31
(zitiert als: Hesse/Peylo et al., Potenziale für ein industrieübergreifendes Flottenlernen, S.)

Hevers, Erik
Informationszugangsansprüche des forschenden Wissenschaftlers, Berlin 2015

Hoeren, Thomas
Ein Treuhandmodell für Autodaten? – § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion
Neue Zeitschrift für Verkehrsrecht, Heft 4/2018, S. 153-155
(zitiert als: Hoeren, Ein Treuhandmodell für Autodaten? – § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch-

	oder vollautomatisierter Fahrfunktion, NZV 2018, Nennung Anfangsseite, Zitatseite)
Hummel, Patrick; Braun, Matthias; Augsberg, Steffen; von Ulmenstein, Ulrich; Dabrock, Peter	Datensouveränität - Governance-Ansätze für den Gesundheitsbereich Cham 2021, S. 1-41 (zitiert als: Hummel/Braun/Augsberg/von Ulmenstein/Dabrock, Datensouveränität - Governance-Ansätze für den Gesundheitsbereich, 2021, S.)
Isensee, Josef; Kirchhof, Paul	Handbuch des Staatsrechts: Band VIII, Grundrechte: Wirtschaft, Verfahren, Gleichheit 3. Auflage, Heidelberg 2010 (zitiert als: Bearbeiter, Titel, in Isensee/Kirchhof, Handbuch des Staatsrechts: Band VIII, Grundrechte: Wirtschaft, Verfahren, Gleichheit, 3. Auflage, 2010, § Rn.)
Jarass, Hans D.	Charta der Grundrechte der Europäischen Union: GRCh 4. Auflage, München 2021 (zitiert als: Bearbeiter, in: Jarass, EU-Grundrechte-Charta, 4. Auflage, 2021, Art. Rn.)
Kerber, Wolfgang; Gill, Daniel	Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation Journal of Intellectual Property, Information Technology and E-Commerce Law, Heft 10 (2)/2019, S. 244-256 (zitiert als: Kerber/Gill, Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, JIPITEC 2019, Nennung Anfangsseite, Zitatseite)
Knauer, Christoph; Kudlich, Hans; Schneider, Hartmut	Münchner Kommentar zur Strafprozessordnung 1. Auflage, München 2014 (zitiert als: Bearbeiter, in: Knauer/Kudlich/Schneider, MüKo StPO, 1. Auflage, 2014, § 476 Rn. 1;
Kollmar, Frederike; El Auwad, Maya	Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen Kommunikation & Recht, Heft 2/2021, S. 73-78 (zitiert als: Kollmar/El Auwad, Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen, K&R 2021, Nennung Anfangsseite, Zitatseite)
Körner, Anne; Mutschler, Bernd; Leitherer, Stephan;	Kasseler Kommentar Sozialversicherungsrecht 112. Ergänzungslieferung, München 2020

Rolfs, Christian
(zitiert als: Bearbeiter, in: Körner/Mutschler/Leitherer/Rolfs, Kasseler Kommentar Sozialversicherungsrecht, 112. Ergänzungslieferung, 2020, § Rn.)

Kühling, Jürgen
Der datenschutzrechtliche Rahmen für Datentreuhänder
Zeitschrift für Digitalisierung und Recht, Heft 1/2021, S. 1-26
(zitiert als: Kühling, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, Nennung Anfangsseite, Zitatseite)

Kühling, Jürgen;
Buchner, Benedikt
Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG
3. Auflage, München 2020
(zitiert als: Bearbeiter, in: Kühling/Buchner, DSGVO/BDSG, 3. Auflage, 2020, Art. Rn.)

Lang, Markus
TTDSG – Neuregelung des Datenschutzes in den Bereichen Telekommunikation und Telemedien geplant
Kommunikation & Recht, Heft 11/2020, S. 714-719
(zitiert als: Lang, TTDSG – Neuregelung des Datenschutzes in den Bereichen Telekommunikation und Telemedien geplant, K&R 2020, Nennung Anfangsseite, Zitatseite)

Lauber-Rönsberg, Anne;
Krahn, Philipp;
Baumann, Paul
Gutachten zu den rechtlichen Rahmenbedingungen des Forschungsdatenmanagements im Rahmen des DataJus-Projektes
Dresden 2018, S. 1-20
(zitiert als: Lauber-Rönsberg/Krahn/Baumann, Kurzfassung: Gutachten zu den rechtlichen Rahmenbedingungen des Forschungsdatenmanagements, 2018, S. 16,

Lehne, Moritz;
Sass, Julian;
Essenwanger, Andrea;
Schepers, Josef;
Thus, Sylvia
Why digital medicine depends on interoperability
nature partner journals Digital Medicine 2, 79 (2019), S. 1-5
(zitiert als: Lehne/Sass/Essenwanger/Schepers/Thus, Why digital medicine depends on interoperability, npj Digital Medicine, 2019, S.)

Liesching, Marc
Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG
Multimedia und Recht, Heft 1/2018, S. 26-30
(zitiert als: Liesching, Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG, MMR 2018, Nennung Anfangsseite, Zitatseite)

Liesching, Marc
Das Herkunftslandprinzip der E-Commerce-Richtlinie und seine Auswirkung auf die aktuelle Mediengesetzgebung in Deutschland
Berlin 2020, S. 1-145
(zitiert als: Liesching, Das Herkunftslandprinzip der E-Commerce-Richtlinie und seine Auswirkung auf die aktuelle Mediengesetzgebung in Deutschland, 2020, S.)

Meyer, Jürgen;
Hölscheidt, Sven
Charta der Grundrechte der Europäischen Union
5. Auflage, Baden-Baden 2019
(zitiert als: Bearbeiter, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage, 2019, Art. Rn.)

Möllers, Thomas M. J.
Juristische Methodenlehre
2. Auflage, München 2019
(zitiert als: Möllers, Juristische Methodenlehre, 2. Auflage, 2019, § Rn.)

Mundhenke, Jens
Wettbewerbswirkungen von Open-Source-Software und offenen Standards auf Softwaremärkten
Kieler Studien 338
Heidelberg 2007, S. 1-280
(zitiert als: Mundhenke, Wettbewerbswirkungen von Open-Source-Software und offenen Standards auf Softwaremärkten, 2007, S.)

Nölscher, Patrick
Das Netzwerkdurchsetzungsgesetz und seine Vereinbarkeit mit dem Unionsrecht
Zeitschrift für Urheber- und Medienrecht, Heft 4/2020, S. 301-312
(zitiert als: Nölscher, Das Netzwerkdurchsetzungsgesetz und seine Vereinbarkeit mit dem Unionsrecht, ZUM 2020, Nennung Anfangsseite, Zitatseite)

Office of the Information & Privacy Commissioner for British Columbia
Access to Data for Health Research
Victoria 2018, S. 1-15
(zitiert als: Office of the Information & Privacy Commissioner for British Columbia, Access to Data for Health Research, 2018, S.)

Ohly, Ansgar
„Volenti non fit iniuria“ - Die Einwilligung im Privatrecht
Jus Privatum 73, Tübingen 2002, S. 1-503
(zitiert als: Volenti non fit iniuria - Die Einwilligung im Privatrecht
2002, S.)

Paal, Boris;
Pauly, Daniel A.
Datenschutz-Grundverordnung
Bundesdatenschutzgesetz: DS-GVO/BDSG
3. Auflage, München 2021

(zitiert als: Bearbeiter, in: Paal/Pauly, DSGVO, 3. Auflage, 2021, Art. Rn.)

Peifer, Karl-Nikolaus Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Zivilrechtliche Aspekte
Zeitschrift für das gesamte Medienrecht/Archiv für Presserecht, Heft 1/2018, S. 14-22
(zitiert als: Peifer, Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Zivilrechtliche Aspekte, AfP 2018, Nennung Anfangsseite, Zitatseite)

Pigeot, Iris;
Buchner, Benedikt Epidemiologie und Datenschutz
Datenschutz und Datensicherheit, Heft 12/2014, S. 816-820
(zitiert als: Pigeot/Buchner, Epidemiologie und Datenschutz, DuD 2014, Nennung Anfangsseite, Zitatseite)

Podszun, Rupprecht Handwerk in der digitalen Ökonomie, Baden-Baden 2021

Putnings, Markus;
Neuroth, Heike;
Neumann, Janna Praxishandbuch Forschungsdatenmanagement
Berlin 2021, S. 1-587
(zitiert als: Bearbeiter, Titel, in: Putnings/Neuroth/Neumann, Praxishandbuch Forschungsdatenmanagement, 2021, S.)

Rat für Informationsinfrastrukturen, Herausforderung Datenqualität - Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel
2. Auflage, Göttingen 2020, S. 1-168
(zitiert als: Rat für Informationsinfrastrukturen, Herausforderung Datenqualität - Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel, 2020, S.)

Rathke, Kurt-Dietrich Lebensmittelrecht
178. Ergänzungslieferung, München 2020
(zitiert als: Bearbeiter, in: Zipfel/Rathke, LebensmittelR, 178. Ergänzungslieferung, 2020, § Rn.)

Recker Jonas;
Helbig, Kerstin;
Neumann, Janna Zertifizierung von Forschungsdatenrepositorien: Wege, Praxiserfahrungen und Perspektiven - 10. Workshop der DINI/nestor-AG Forschungsdaten Empfehlungen und Erfahrungsberichte für die Praxis von Forschungsdatenmanagerinnen und -managern, Nr. 2/2020, S. 97-105

(zitiert als: Recker/Helbig/Neumann, Zertifizierung von Forschungsdatenrepositorien - Wege, Praxiserfahrungen und Perspektiven, Bausteine Forschungsdatenmanagement: Empfehlungen und Erfahrungsberichte für die Praxis von Forschungsdatenmanagerinnen und -managern 2020, Nennung Anfangsseite, Zitatseite)

Richter, Heiko
„Open Government Data“ für Daten des Bundes
Neue Zeitschrift für Verwaltungsrecht, Heft 19/2017, S. 1401-1413
(zitiert als: Richter, „Open Government Data“ für Daten des Bundes, NVwZ 2017, Nennung Anfangsseite, Zitatseite)

Roßnagel, Alexander
Handbuch Datenschutzrecht
1. Auflage, München 2003
(zitiert als: Bearbeiter, in: Roßnagel, Handbuch Datenschutzrecht, 1. Auflage, 2003, Kap. Rn.)

Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen
Digitalisierung für Gesundheit: Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems (Gutachten 2021)
Berlin 2021, S. 1-363
(zitiert als: Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen, Digitalisierung für Gesundheit: Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, 2021, S.)

***Sandys* et al.**
A strategy for a Modern Digitalised Energy System Energy - Data Taskforce report
London 2019, S. 1-56
(zitiert als: Sandys et al., A strategy for a Modern Digitalised Energy System Energy, Data Taskforce report, 2019, S.)

Schwartmann, Rolf
Gesetzesrecht vor Hausrecht - Die geplanten Änderungen des NetzDG
Multimedia und Recht, Heft 8/2020, S. 501-502
(zitiert als: Schwartmann, Gesetzesrecht vor Hausrecht - Die geplanten Änderungen des NetzDG, MMR 2020, Nennung Anfangsseite, Zitatseite)

Schwartmann, Rolf; Benedikt, Kristin; Reif, Yvette
Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz?
Multimedia und Recht, Heft 2/2021, S. 99-102
(zitiert als: Schwartmann/Benedikt/Reif, Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz?, MMR 2021, Nennung Anfangsseite, Zitatseite)

Schwartmann, Rolf;
Hanloser, Stefan;
Weiß, Steffen
PIMS im TTDSG, Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz, Kurzgutachten im Auftrag der European netID Foundation, Stiftung Datenschutz, Neue Wege bei der Einwilligung
2021, S. 1-10
(zitiert als: Schwartmann/Hanloser/Weiß, PIMS im TTDSG, Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz, Kurzgutachten im Auftrag der European netID Foundation, Stiftung Datenschutz, Neue Wege bei der Einwilligung, S.)

Slokenberga, Santa;
Tzortzatou, Olga;
Reichel, Jane
GDPR and Biobanking
Law, Governance and Technology Series, Volume 43, Cham 2021, S. 1-434
(zitiert als: Bearbeiter, Titel, in: Slokenberga/Tzortzatou/Reichel, GDPR and Biobanking, Law, Governance and Technology Series, Volume 43, 2021, S.)

Specht-Riemenschneider, Louisa;
***Blankertz, Aline* et al.**
Die Datentreuhand
Multimedia und Recht, Beilage Heft 6/2021, S. 25-48
(zitiert als: Specht-Riemenschneider/Blankertz et al., Die Datentreuhand, MMR-Beilage 2021, Nennung Anfangsseite, Zitatseite)

Specht-Riemenschneider, Louisa;
Radbruch, Alexander
Datennutzung und -schutz in der Medizin: Forschung braucht Daten
Deutsches Ärzteblatt, 118/2021, S. 27-28
(zitiert als: Specht-Riemenschneider/Radbruch, Datennutzung und -schutz in der Medizin: Forschung braucht Daten, Deutsches Ärzteblatt 118/2021, Nennung Anfangsseite, Zitatseite)

Specht, Louisa
Das Verhältnis möglicher Datenrechte zum Datenschutzrecht
Gewerblicher Rechtsschutz und Urheberrecht International, Heft 12/2017, S. 1040-1047
(zitiert als: Specht, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, Nennung Anfangsseite, Zitatseite)

Specht, Louisa;
Mantz, Reto
Handbuch Europäisches und deutsches Datenschutzrecht
1. Auflage, München 2019
(zitiert als: Bearbeiter, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage, 2019, § Rn.)

Spindler, Gerald
Das Netzwerkdurchsetzungsgesetz
Kommunikation & Recht, Heft 9/2017, S. 533-544

(zitiert als: Spindler, Das Netzwerkdurchsetzungsgesetz, K&R 2017, Nennung Anfangsseite, Zitatseite)

Spindler, Gerald Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz – europarechtswidrig?
Zeitschrift für Urheber- und Medienrecht, Heft 6/2017, S. 473-487
(zitiert als: Spindler, Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz – europarechtswidrig?, ZUM 2017, Nennung Anfangsseite, Zitatseite)

Spindler, Gerald Rechtsdurchsetzung von Persönlichkeitsrechten
Gewerblicher Rechtsschutz und Urheberrecht, Heft 4/2018, S. 365-373
(zitiert als: Spindler, Rechtsdurchsetzung von Persönlichkeitsrechten, GRUR 2018, Nennung Anfangsseite, Zitatseite)

Strech, Daniel;
Graf von Kielmannsegg, Sebastian;
Zenker, Sven;
Krawczak, Michael;
Semler, Sebastian C. „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen
Berlin 2020, S. 1-141
(zitiert als: Strech/von Kielmannsegg/Zenker/Krawczak/Semler, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, 2020, S.)

Sydow, Gernot Europäische Datenschutzgrundverordnung,
2. Auflage, Baden-Baden 2018
(zitiert als: Bearbeiter, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Auflage, 2018, Art. Rn.)

Taeger, Jürgen DSGVO und BDSG, 3. Auflage, Frankfurt 2019
(zitiert als: Bearbeiter, in: Taeger/Gabel, DSGVO BDSG, 3. Auflage, 2019, DSGVO Art. Rn.)

Veil, Winfried Datenaltruismus: Wie die EU-Kommission eine gute Idee versemmelt, CR-Online Blog v. 01.12.2020, abrufbar unter https://www.cr-online.de/blog/2020/12/01/datenaltruismus-wie-die-eu-kommission-eine-gute-idee-versemmelt/, zuletzt abgerufen am 16.07.2021

Verbraucherzentrale Bundesverband Personal Information Management Systems (PIMS)
Berlin 2020, S. 1-12
(zitiert als: Verbraucherzentrale Bundesverband, Personal Information Management Systems (PIMS), 2020, S.)

***Vermeir, Koen* et al.**
Global Access to Research Software: The Forgotten Pillar of Open Science Implementation
Global Young Academy, Halle 2018, S. 1-75
(zitiert als: Vermeir et al., Global Access to Research Software: The Forgotten Pillar of Open Science Implementation, Global Young Academy, 2018, S.)

von der Groebe, Hans;
Schwarze, Jürgen;
Hatje, Armin
Europäisches Unionsrecht
7. Auflage, Baden-Baden 2015
(zitiert als: Bearbeiter, in: von der Groebe/Schwarze/Hatje, Europäisches Unionsrecht, 7. Auflage, 2015, Art. Rn.)

von Landmann, Robert (Begr.);
Rohmer, Gustav (Begr.)
Umweltrecht: UmweltR
94. Ergänzungslieferung, München 2021
(zitiert als: Bearbeiter, in: Landmann/Rohmer, UmweltR, 94. Ergänzungslieferung, 2020, § Rn.)

von Mangoldt, Hermann;
Klein, Friedrich;
Starck, Christian
Kommentar zum Grundgesetz
5. Auflage, München 2005
(zitiert als: Bearbeiter, in: v. Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, 5. Auflage, 2005, Art. Rn.)

Wagner Bernd;
Goebele, Thilo
Freie Fahrt für das Auto der Zukunft?
Kritische Analyse des Gesetzentwurfs zum hoch- und vollautomatisierten Fahren
Zeitschrift für Datenschutz, Heft 6/2017, S. 263-269
(zitiert als: Wagner/Goebele, Freie Fahrt für das Auto der Zukunft?, ZD 2017, Nennung Anfangsseite, Zitatseite)

Wielsch, Dan
Zugangsregeln – Die Rechtverfassung der Wissensteilung, Tübingen 2008.

***Wilkinson, Mark D.* et al.**
Comment: The FAIR Guiding Principles for scientific data management and stewardship
Nature - Scientific Data (3), 2016, S. 1-9
(zitiert als: Wilkinson et al., Comment: The FAIR Guiding Principles for scientific data management and stewardship, Nature - Scientific Data, 2016, S.)

Wischmeyer, Thomas;
Herzog, Eva
Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte
Neue Juristische Wochenschrift, Heft 5/2020, S. 288-293
(zitiert als: Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, NJW 2020, Nennung Anfangsseite, Zitatseite)

Wissenschaftliche Dienste des Deutschen Bundestages
Die Wissenschaftsfreiheit im Grundgesetz und in der Charta der Grundrechte der Europäischen Union

Ausarbeitung, Berlin 2010, S. 1-13
(zitiert als: Wissenschaftliche Dienste des Deutschen Bundestages, Die Wissenschaftsfreiheit im Grundgesetz und in der Charta der Grundrechte der Europäischen Union, Ausarbeitung, S.)

Wissenschaftsrat
Zum Wandel in den Wissenschaften durch datenintensive Forschung
Positionspapier, Köln 2020, S. 1-72
(zitiert als: Wissenschaftsrat, Zum Wandel in den Wissenschaften durch Daten intensive Forschung, Positionspapier, 2020, S.)

Wolter, Jürgen
Systematischer Kommentar zur Strafprozessordnung: SK-StPO
5. Auflage, Köln 2017
(zitiert als: Bearbeiter, in: Wolter, SK-StPO, 5. Auflage, 2017, § Rn.)

Zech, Herbert
Information als Schutzgegenstand
Jus Privatum 166, Tübingen 2012, S. 1-488
(zitiert als: Zech, Information als Schutzgegenstand, 2012, S.)

Zimmermann, Judith
Zum Potenzial des europäischen Weiterverwendungsrechts für die Erforschung der Biodiversität
Zeitschrift für Umweltrecht, Heft 2/2021, S. 84-92
(zitiert als: Zimmermann, Zum Potenzial des europäischen Weiterverwendungsrechts für die Erforschung der Biodiversität, ZUR 2021, Nennung Anfangsseite, Zitatseite)

XIV. Danksagung

Für die zahlreichen Gespräche im Vorfeld sowie während der Erstellung dieses Gutachtens möchte ich ganz herzlich danken:

Lucie Arntz, Gerd Billen, Aline Blankertz, Paul Heidhues, Jana Holland, Wolfgang Kerber, Sebastian Louven, Susanne Möhring, Walter Pasquarelli, Alexander Radbruch, Bertram Raum, Monika Schnitzer, Nick Schneider, Gert G. Wagner, Alexander Wehde, Nikola und Susanne Werry, Winfried Veil sowie Thomas Wischmeyer. Wie üblich, bin ich nicht allen Rat- und Vorschlägen gefolgt.