**Deutscher Bundestag**
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)109

UNIVERSITÄT BONN
Rechts- und Staatswissenschaftliche Fakultät
Rechtswissenschaft

RHEINISCHE
FRIEDRICH-WILHELMS-
UNIVERSITÄT BONN

UNIVERSITÄT BONN · Prof. Dr. L. Specht · Adenauerallee 24-42, 53113 Bonn

An den Ausschuss Digitale Agenda
z.Hd. des Vorsitzenden
MdB Manuel Höferlin
Deutscher Bundestag
Platz der Republik
110117 Berlin

**Prof. Dr. Louisa Specht-Riemenschneider**

Lehrstuhl für Bürgerliches Recht,
Informations- und Datenrecht

Adenauerallee 24-42
53113 Bonn

T 0228/73-4240
F 0228/73-5741
E Louisa.Specht@Forschungsstelle-Datenrecht.de

Sekretariat: Jacqueline Götsche

T 0228/73-4240
F 0228/73-5741
E sekretariat.specht@jura.uni-bonn.de

Bonn, 18.02.2021

**Öffentliche Anhörung des Ausschusses Digitale Agenda**
**am 24. Februar 2021 zum Thema „Datenstrategie der Bundesregierung“ (BT-Drs. 19/26450) verbunden mit „Eckpunkte einer Datenstrategie der Bundesregierung“(BT-Drs. 19/16075) und dem Antrag der Fraktion der FDP „Datenpolitik für Selbstbestimmung, Wettbewerb und Innovation“ (BT-Drs. 19/26538)**

Wir SEIT 200 JAHREN

www.200jahre.uni-bonn.de

Sehr geehrte Mitglieder des Ausschusses Digitale Agenda,

der Ausschussvorsitzende MdB M. Höferlin hat mich durch Schreiben vom 03.02.2021 eingeladen, an der o.g. öffentlichen Anhörung als Expertin teilzunehmen. Dieser Einladung komme ich gerne nach. Zur Vorbereitung wurde mir am 16.02.2021 der interfraktionelle Fragebogen zugesandt. Im Folgenden würde ich gerne vorab schriftlich zu einigen der hier aufgeworfenen Fragen

Universitätskasse Bonn:

Sparkasse KoelnBonn
BIC: COLSDE 33
IBAN: DE08370501980000057695

USt.-Id-Nr.:
DE 122 119 125

Stellung nehmen. Auch wenn ich sämtliche Aspekte der Datenstrategie mit Interesse verfolge, berühren doch v.a. spezifische Fragen im Themenblock „Datennutzung“ den Schwerpunkt meiner Forschungstätigkeit. Ich erlaube mir daher nach Rücksprache mit dem Ausschussvorsitzenden, meine Stellungnahme auf Fragen in diesem Themenblock zu beschränken.

Ich wäre Ihnen dankbar, wenn Sie die nachfolgende Stellungnahme zur Kenntnis nehmen würden. Bei der öffentlichen Anhörung beantworte ich gerne weitergehende Fragen zum Themenbereich der Datennutzung.

Mit freundlichen Grüßen

Louisa Specht-Riemenschneider

**Stellungnahme zum Thema**

**„Datenstrategie der Bundesregierung“ (BT-Drs. 19/26450) verbunden mit**

**„Eckpunkte einer Datenstrategie der Bundesregierung“(BT-Drs. 19/16075)**

**und**

**dem Antrag der Fraktion der FDP „Datenpolitik für Selbstbestimmung, Wettbewerb und Innovation“ (BT-Drs. 19/26538)**

**- Zusammenfassung -**

1. **Fehlende Datenzugangsgewährung hat im Wesentlichen drei Gründe:**
   a) **Fehlende materiell-rechtliche Datenzugangsansprüche**
   b) **Fehlende institutionelle und technische Lösungen zur Datenzugangsgewährung (Datentreuhandmodelle)**
   c) **Rechtsunsicherheit v.a. im Bereich des Datenschutzrechts.**

2. **Bei der Normierung neuer Datenzugangsansprüchen ist eine Lösung zu suchen, die die Rechte und Interessen sowohl der zugangsbeanspruchenden als auch der datenhaltenden Personen in Ausgleich bringt. Beide Interessen können grundrechtlich geschützt sein und durch die (fehlende) Datenzugangsgewährung empfindlich berührt werden.**

3. **Datenzugangsansprüche sollten nicht horizontal, sondern grundsätzlich sektorspezifisch und allein auf Grundlage eines tatsächlichen Bedarfs vorgesehen werden.**

4. **Neben diese sektorspezifischen Datenzugangsansprüche sollten zweckgebundene intersektorale Datenzugangsansprüche für die Wissenschaft treten, deren Umfang und Grenzen bestimmt und die im**

**Rahmen eines „Gesetzes für Forschungsdatenschutz und Forschungsdatenzugang“ ausgestaltet werden.**

5. **Datentreuhandmodelle haben das Potential, eine Vielzahl von Problemen zu lösen, die derzeit im Kontext der Datenwirtschaft auftreten. Sie können z.B. das freiwillige Datenteilen in geschützten Räumen ermöglichen und (in Form von PIMS) zur Effektivierung des Datenschutzrechts beitragen. Darüber hinaus können sie eine wesentliche Rolle z.B. für das Trainieren Künstlicher Intelligenzen mit den geteilten Daten oder auch für die Anonymisierung und Pseudonymisierung von Datenbeständen einnehmen. Sie sind aber vielgestaltig möglich, einendes Merkmal ist allein die Datenzugangsmittelung im Fremdinteresse. Vor einer Regulierung sollten Datentreuhandmodelle daher systematisiert und je nach Modell auf ihren Regulierungsbedarf untersucht werden. One-size-fits-all Lösungen sollten vermieden werden. Insgesamt ist eine ermöglichende, anreizbasierte Regulierung statt zusätzlicher bürokratischer Anforderungen wünschenswert.**

6. **Datentreuhandlösungen benötigen außerdem einen sicheren Rechtsrahmen. Dies gilt v.a. mit Blick auf das Datenschutzrecht. Die Erklärung der datenschutzrechtlichen Einwilligung, ihr Widerruf und die Ausübung von Betroffenenrechten sollten im Wege der Stellvertretung möglich sein. Aus Rechtssicherheitserwägungen heraus sollte dies im Gesetz vorgesehen werden.**

7. **Der Umgang mit nicht-personenbezogenen Daten sollte erleichtert werden. Für sie gilt der Grundsatz der Datenminimierung nicht. Häufig herrscht aber Rechtsunsicherheit darüber, wann ein Datum personenbezogen ist und wie mit Mixed-Data Sets zu verfahren ist. Hier sollten**

**Anreize zur Entwicklung von Anonymisierungslösungen gegeben werden. Sinnvoll scheint die Entwicklung von Standards zur Anonymisierung, bei deren Einhaltung die Anonymisierung unwiderleglich vermutet wird.**

8. **Auch eine Anonymisierung erfordert es aber, dass Daten zunächst kurzweilig erhoben und gespeichert werden, bevor sie unmittelbar nach der Anonymisierung wieder gelöscht werden. Die Gefährdung des informationellen Selbstbestimmungsrechtes scheint bei dieser äußerst kurzweiligen Datenspeicherung zumindest bei Einhaltung entsprechender IT-Sicherheitsstandards gering. Zu Zwecken einer Anonymisierung und anschließenden Nutzbarkeit der Daten frei von datenschutzrechtlichen Vorgaben sollte daher ein zusätzlicher Erlaubnistatbestand entsprechend § 44a UrhG geschaffen werden, der die hierfür erforderliche kurzweilige Datenspeicherung gestattet.**

**Stellungnahme zum Thema**

**„Datenstrategie der Bundesregierung“ (BT-Drs. 19/26450) verbunden mit**

**„Eckpunkte einer Datenstrategie der Bundesregierung“(BT-Drs. 19/16075)**

**und**

**dem Antrag der Fraktion der FDP „Datenpolitik für Selbstbestimmung, Wettbewerb und Innovation“ (BT-Drs. 19/26538)**

- Ausführliche Fassung -

(Themenblock Datennutzung)

## A. Grundlegendes

Der Umgang mit personenbezogenen und nicht-personenbezogenen Daten prägt Wirtschaft, Wissenschaft, Gesellschaft und Politik heute mehr denn je. Die juristische Diskussion fokussierte sich dabei lange Jahre auf die Frage nach Ausschließlichkeitsrechten an Daten,[1] hat sich zwischenzeitlich aber auf die Frage nach Datenzugangsansprüchen verlagert.[2] Derartige Datenzugangsansprüche existieren außerhalb der DS-GVO de lege lata allenfalls sektorspezifisch, z.B. für

[1] Exemplarisch *Zech*, Information als Schutzgegenstand, Tübingen 2012; *Specht*, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, S. 288-296; *Boerding et al*, Data Ownership – A Property Rights Approach from a European Perspective, 11 J. Civ. L. Stud. 2018, S. 325-369; *Richter/Hilty*, Die Hydra des Dateneigentums – eine methodische Betrachtung, Max Planck Institute for Innovation & Competition Discussion Paper No.12 (2018), abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3263404; zuletzt *Kühling/Sackmann*, Irrweg „Dateneigentum, ZD 2020, S. 24-30.

[2] *Drexl* et al, Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate, Max Planck Institute for Innovation & Competition Discussion Paper No.16-10 (2016), abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165.

Finanzdienstleistungen[3] oder für Fahrzeugdaten zwecks Reparaturmaßnahmen.[4] Art. 16 Abs. 4 Digitale-Inhalte Richtlinie[5] und seine Umsetzung in § 327p Abs. 3 S. 1 BGB Ref-E sieht einen Datenzugangsanspruch für nicht-personenbezogene Daten bei Vertragsbeendigung vor, dessen Anwendungsbereich allerdings äußerst gering sein dürfte. Berechtigten Forderungen nach einer überschießenden Umsetzung der Richtlinie wurde nicht entsprochen.[6] Für Daten der öffentlichen Verwaltung finden sich vor allem Offenlegungspflichten.[7] Innerhalb der DS-GVO existieren Datenzugangsansprüche in Art. 20 DS-GVO als Datenportabilitätsrecht sowie in Art. 15 DS-GVO in Form des Auskunftsanspruchs. Sie berechtigen einzig den Betroffenen. Ob sie auch durch Dritte ausgeübt werden können, ist streitig (dazu sogleich unter B.III.5. und 6.), was maßgeblich zur Ineffizienz beider Ansprüche beiträgt. Wettbewerbsrechtliche Zugangsansprüche knüpfen in der Regel an eine marktbeherrschende Stellung sowie weitere Vo-

[3] Art. 38-60 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt.

[4] Art. 61-66 Verordnung (EU) 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, zur Änderung der Verordnungen; Für einen Überblick über sektorspezifische Zugangsansprüche vgl. *Graef/Husovec/van den Boom*, Spill-overs in data governance: Uncovering the uneasy relationship between the GDPR's right to data portability and EU sector-specific data access regimes, EuCML 2020, S. 3-16.

[5] Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen.

[6] *Metzger*, Stellungnahme zur öffentlichen Anhörung des Ausschusses Digitale Agenda am 28. Okober 2020 zu GAIA X, Datenräume, Datenstrategie, Berlin 2020, S. 9 ff., abrufbar unter: https://www.bundestag.de/resource/blob/801254/eaa4faba3dfcb36dfd9b504034d51233/Stellungnahme-Dr-Metzger-data.pdf.

[7] Zu nennen sind bspw. § 12a EGovG, § 11 IFG und §§ 7 Abs.1, 10 UIG, wobei Offenlegungspflichten derzeit überschaubar sind und grds. kein subjektiv-öffentliches Recht des Einzelnen begründen. Unlängst mehren sich aber Bestrebungen, diese Pflichten auszuweiten, vgl. dazu bspw. den nationalen Aktionsplan der Bundesregierung zur Umsetzung der Open-Data-Charta der G8, abrufbar unter: https://www.bmvg.de/resource/blob/20686/55536214b782b9d04c7ae29b0f12c29a/g-01-nationaler-aktionsplan-open-data-data.pdf.

raussetzungen an und können dementsprechend ebenfalls nur einen sehr geringen Teilbereich erforderlicher Datenzugangsansprüche erfassen. Insgesamt sind Datenzugangsansprüche de lege lata unterentwickelt.

Bei der Ausgestaltung derartiger Datenzugangsansprüche ist freilich stets eine grundrechtskonforme Lösung zu finden, denn nicht nur der Zugriff auf Datenbestände kann von einem grundrechtlich geschützten Interesse, z.B. der Wissenschafts- und Forschungsfreiheit, Art. 5 Abs. 3 GG, getragen sein. Die Datenbestände der zur Zugangsgewährung verpflichteten Unternehmen sind häufig über den Geschäftsgeheimnisschutz oder auch über das Urheberrecht, Art. 14 GG, geschützt. Sind personenbezogene Daten Gegenstand eines Datenzugangsanspruchs, so ist das informationelles Selbstbestimmungsrecht der Betroffenen, Art. 2 Abs. 1, 1 Abs. 1 GG, zu beachten.[8]

Datenzugangsansprüche aber sind freilich nur dort erforderlich, wo ein Marktversagen festzustellen ist und ein Datenteilen daher nicht bereits auf freiwilliger Grundlage Erfolg verspricht. Ist ein freiwilliges Datenteilen aber so gut wie gar nicht feststellbar, wie dies derzeit der Fall ist, liegt dies nicht überall daran, dass die maßgeblichen Akteure nicht willens sind, die bei ihnen gespeicherten Daten mit anderen zu teilen. Häufig fehlt es Institutionen schlicht an der faktischen Möglichkeit sowie der erforderlichen Rechtssicherheit.

Denn Datenteilen erfordert einheitliche Datenstandards, technische Grundvoraussetzungen zur Übermittlung der teils erheblichen Datenbestände, institutionelle Lösungen zum vertrauensvollen Umgang mit Daten (Datentreuhandsysteme, zu denen auch PIMS gehören), und einen Rechtsrahmen, der eindeutige

[8] Zur grundrechtlichen Dimension von Datenzugangsrechten *Wischmeyer/Herzog*, Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, NJW 2020, S. 288-293.

Aussagen über Zulässigkeit und Bedingungen des Datenteilens trifft. An all dem fehlt es bislang.

## B. Lösungsoptionen

Fehlende Datenzugangsgewährung hat also im Wesentlichen drei Gründe:

1. Fehlende materiell-rechtliche Datenzugangsansprüche
2. Fehlende institutionelle und technische Lösungen zur Datenzugangsgewährung (Datentreuhandmodelle)
3. Rechtsunsicherheit v.a. im Bereich des Datenschutzrechts aber auch in Bezug auf sonstige Schutzrechte (auch nicht-personenbezogener Daten) wie den Geschäftsgeheimnisschutz und das Urheberrecht

Die von der Datenstrategie der Bundessregierung identifizierten Probleme lassen sich im Themenblock „Datennutzung“ vornehmlich unter diese drei Gründe fassen, weshalb die nachfolgenden Ausführungen in ihrem Sinne systematisiert werden sollen. Insgesamt bietet die Datenstrategie der Bundesregierung vorsichtige Lösungsoptionen an, die häufig aber noch durch weitere Prüfung und Wissenschaftsförderung konkretisiert werden müssen. Sie sollen im Folgenden bewertet und ergänzt werden.

### I. Fehlende materiell-rechtliche Datenzugangsansprüche

Bei der Normierung von Datenzugangsansprüchen ist zunächst die Frage zu beantworten, ob es bei sektorspezifischen Lösungen bleiben und diese ggf. auszubauen sind oder ob es horizontale Datenzugangsansprüche geben sollte. Die Datenstrategie der Bundesregierung formuliert eine vorsichtige Tendenz zu sektorspezifischen Regelungen, die neben kartellrechtliche Zugangsansprüche tre-

ten sollen. Dem ist jedenfalls insoweit zuzustimmen, als eine Datenteilungspflicht für jedermann nicht der richtige Weg ist. Ein solcher „One Size fits all-Ansatz“ berücksichtigt die grundrechtlich geschützten Interessen der Dateninhaber nicht angemessen. Sektorspezifischen Lösungen ist damit grundsätzlich der Vorzug zu geben.

Die in der Datenstrategie vorgeschlagenen Maßnahmen sind indes längst nicht ausreichend. Es bedarf darüber hinaus:

**1. Horizontaler Vorgaben für die Umsetzung von Datenzugangsansprüchen**

**2. Zweckgebundener intersektoraler Datenzugangsansprüche**

Horizontal formuliert werden müssen indes Datenstandards und Anforderungen an Schnittstellen, damit eine Datenzugangsgewährung dort, wo sie sektorspezifisch oder zweckgebunden intersektoral vorgegeben wird, auch tatsächlich funktioniert. Mit derart horizontalen Vorgaben für die Umsetzung sämtlicher Datenzugangsansprüche lassen sich auch intersektorale Zugangsansprüche verwirklichen, z.B. indem Angehörige des Gesundheitssektors zu Forschungszwecken Zugang zu Lebensmitteldaten aus dem Ernährungssektor erhalten. Derart zweckgebundene intersektorale Datenzugangsansprüche sollten ebenfalls zwingend mitbedacht werden. Es bedarf einer politischen Entscheidung darüber, für welche Zwecke ein solcher intersektoraler Datenzugang ermöglicht werden soll. Der hier an erster Stelle zu privilegierende Zweck ist die auch bereits im Datenschutzrecht in hervorgehobener Stellung auftretende Forschung. Ein möglicher Weg wäre es, ihr überall dort Datenzugang zu gewähren, wo bereits Datenzugangsansprüche anderer Akteure bestehen, (abgeleitete Datenzugangsansprüche). Auch darüber hinaus ist aber zu erwägen, wo eine Notwendigkeit für wissenschaftsbezogene Datenzugangsansprüche besteht. Eine Reihe von Datenzugangsansprüchen zugunsten der Wissenschaft existiert aber bereits

in Form von Forschungsklauseln. Um zu entscheiden, wo darüber hinaus Datenzugangsansprüche erforderlich sind, bedarf es zunächst einer Bestandsaufnahme über diese bestehenden Datenzugangsansprüche. Erst anschließend können sie bei Vorliegen ökonomischer Evidenz sinnvoll ergänzt werden. Auch der Entwurf für einen Digital Services Act enthält einen Datenzugangsanspruch der Wissenschaft gegen Plattformen, der allerdings nicht unmittelbar von der Wissenschaft, sondern allein über den Koordinator für digitale Dienste am Niederlassungsort oder über die Kommission geltend gemacht werden kann, vgl. Art. 31 Abs. 2 DSA-E. Auch eine rechtsvergleichende Analyse von Datenzugangsansprüchen für die Wissenschaft wäre sicher sinnvoll.

Datenzugangsansprüche der Wissenschaft ließen sich in einem spezifischen Gesetz über den Forschungsdatenschutz und den Forschungsdatenzugang rechtsanwenderfreundlich zusammentragen. Bei der Ausgestaltung von Datenzugangsansprüchen zugunsten der Wissenschaft ist aber unbedingt und v.a. auch über folgende Parameter zu entscheiden:

1. Wer soll Datenzugang erhalten: Der einzelne Wissenschaftler/die einzelne Wissenschaftlerin oder die Wissenschaftsinstitution?
2. Ist eine Vergütung für die Gewährung des Datenzugangs zu zahlen?
3. Welchen Grenzen unterliegen die Datenzugangsansprüche (Geschäftsgeheimnisse, Urheberrechte, Persönlichkeitsrechte, Unmöglichkeit, Unverhältnismäßigkeit etc.?)
4. Welche Anonymisierungs-/Pseudonymisierungsstandards sind einzuhalten, wenn personenbezogene Daten vom Datenzugangsanspruch umfasst werden?
5. Was soll Zugangsgegenstand sein? Zugang zu Rohdaten, Zugang zu aufbereiteten Daten, Zugang zu abgeleiteten Daten?

## II. Fehlende Datentreuhandlösungen

Die Datenstrategie der Bundesregierung adressiert Datentreuhandlösungen u.a. im Kontext verantwortungsvoller Nachnutzung von Daten, im Kontext des Trainings von Anwendung Künstlicher Intelligenzen, im Kontext der Effektivierung datenschutzrechtlicher Befugnisse unter dem Schlagwort „PIMS" sowie explizit unter 2.3 im Kontext des freiwilligen Datenteilens. Diese fehlende Systematik ist symptomatisch für die derzeit auch in rechtlicher Hinsicht geführte Diskussion um mögliche Datentreuhandlösungen. Denn für den Begriff der „Datentreuhand" hat sich eine einheitliche Definition bisher noch nicht herausbilden können.[9] Das hat seinen Grund v.a. darin, dass eine Reihe verschiedener Rechtsverhältnisse unter diesen Begriff gefasst werden. Personal Information Management Systeme (PIMS) in all ihren Erscheinungsformen sollen ebenso darunter fallen wie Drittstellen zur Speicherung von und zur Zugangsgewährung zu personenbezogenen und nicht-personenbezogenen Daten, beispielsweise im Automobilbereich, wo Daten aus dem vernetzten Auto zukünftig nicht mehr (nur?) im Fahrzeug, sondern auch bei einer dritten Stelle gespeichert werden könnten (§ 63a StVG).[10] Ähnliches lässt sich für Mobilitätsdaten aus dem öffentlichen Nahverkehr denken, für medizinische

[9] So auch für Datentreuhandmodelle für personenbezogene Daten *Blankertz*, Designing Data Trusts, S. 13; *Blankertz et al.*, Datentreuhandmodelle – Themenpapier, S. 1; *Schwartmann/Weiß*, Datenmanagement- und Datentreuhandsysteme, S. 19; *Funke*, Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO), S. 6.

[10] Vgl. dazu *RfII*, Datentreuhänder: Potenziale, Erwartungen, Umsetzung – Workshop-Bericht, Februar 2021, S.6, abrufbar unter: http://www.rfii.de/download/rfii-workshopbericht-datentreuhaender-potenziale-erwartungen-umsetzung-februar-2021/; die Forderung nach einem Datentreuhänder schon früher *Gesamtverband der deutschen Versicherungsgesellschaft*, Versicherungswirtschaft „Datenkranz beim automatisierten Fahren gemäß § 63a StVG – externe Speicherung bei einem Datentreuhänder" – Positionspapier, August 2018, abrufbar unter: https://www.gdv.de/resource/blob/36102/c9494add5b56ea558f59204a9f85e914/datentreuhaender-und-automatisiertes-fahren---download-data.pdf.

Forschungsdaten,[11] für die Angaben in digitalen Produktpässen[12] oder für landwirtschaftliche Fahrzeuge, die während des Betriebs Daten, z.B. über die Bodenbeschaffenheit erfassen.[13] Auch ein Daten-Escrow in Analogie zum Software-Escrow wäre eine mögliche Form der Datentreuhand.[14]

Betrachtet man die denkbaren Datentreuhandmodelle genauer, so lässt sich erkennen, dass Datentreuhänder im Wesentlichen die Intermediärsfunktion der Datenzugangsmittelung übernehmen (sollen), und dabei (zumindest auch) im Fremdinteresse handeln (sollen). Die fremdnützige Interessenwahrnehmung ist wesentliches Merkmal der Geschäftsbesorgung nach § 675 BGB und damit auch der zivilrechtlichen Grundlage der Treuhand.[15] Dagegen liegt der Begriffswahl der Datentreuhand ein echtes Treuhandverhältnis im rechtlichen Sinne gerade nicht zugrunde. Schließlich ist die Treuhand im rechtlichen Sinne wesentlich davon geprägt, dass der Treunehmer im Außenverhältnis in der Regel aufgrund einer Vollrechtsübertragung umfangreichere rechtliche Befugnisse hat, als ihm im Innenverhältnis an Befugnissen zuerkannt werden. An Daten aber kann schon mangels ausschließlichkeitsrechtlicher Befugnisse kein Vollrecht übertragen werden. Insoweit scheint für die Begriffsprägung der Datentreuhand allein die Bindung des Datentreuhänders an die Interessen des Datentreugebers entscheidend zu sein. Auch eine doppelseitige Datentreuhand, d.h. eine

[11] Hierher gehören auch die schon lang diskutierten Biodatenbanken, vgl. dazu BT-Drs. 16/5374; *Winickoff/Winickoff*, The Charitable Trust as a Model for Genomic Biobanks, N Engl J Med 349/12 (2003), S. 1180-1184. Exemplarisch sei hier auf die *UK Biobank Ltd.* hingewiesen: https://www.ukbiobank.ac.uk.

[12] So die *Europäische Kommission* im Rahmen ihres „European Green Deal", vgl. Circular Economy Action Plan, März 2020, S. 7, abrufbar unter: https://ec.europa.eu/environment/circular-economy/pdf/new_circular_economy_action_plan.pdf.

[13] Zum Beispiel vgl. *Zech*, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers", CR 2015, S. 137-146, 137.

[14] Eingehend zum Software Escrow *Auer-Reinsdorff/Kast/Dessler* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 38 IT in der Insolvenz, Escrow Rn. 58-105.

[15] Eingehend *Löhnig*, Treuhand: Interessenwahrnehmung und Interessenkonflikt, Tübingen 2006, S. 115 ff.

Bindung sowohl an die Interessen des Treugebers als auch eines anderen ist v.a. dann möglich und vielversprechend, wenn der Treugeber ein Datenverarbeiter ist, der Treuhänder aber nicht nur im Interesse des Datenverarbeiters, sondern auch im Interesse des datenschutzrechtlich Betroffenen tätig werden soll.

Einendes Merkmal jedweder Datentreuhandmodelle ist die Datenzugangsmittelung. Dies gilt sowohl für die PIMS, die dem datenschutzrechtlich Betroffenen Zugang zu den über sie bei Datenverarbeitern gespeicherten Daten mitteln, oder im Falle des Einwilligungsmanagements Datenverarbeitern Zugang zu Daten des Betroffenen verschaffen. Dies gilt aber genauso für die Drittstelle, bei der künftig Daten aus dem vernetzten Auto gespeichert werden könnten oder beim Daten-Escrow.

Für die Entscheidung des Datentreuhänders über die Datenzugangsmittelung ergeben sich zwei Möglichkeiten: Der Datentreuhänder könnte dies nach gesetzlichen (in der Regel noch zu normierenden) Vorgaben entscheiden oder aber aufgrund vertraglicher Vereinbarungen. Der Datentreuhänder könnte die Daten einerseits selbst zentral speichern im Sinne eines Hosting-Dienstes, andererseits aber auch eine autorisierte Person sein, die den Zugang zu dezentral bei anderen Stellen gespeicherten Daten mittelt, die Daten also nur ähnlich einem Cache-Provider (§ 9 TMG) zwecks Übermittlung an einen Dritten zwischenspeichert. Ein ähnliches Modell existiert im australischen Recht für die Gateway-Person im Consumer Data Right.[16]

Aus dem Genannten ergibt sich folgender Definitionsvorschlag: Eine Datentreuhand ist eine natürliche oder juristische Person oder eine Personenhandelsgesellschaft, die den Zugang zu von Dritten bereitgestellten

[16] Section 56BG Competition and Consumer Act. Für eine mögliche Ausgestaltungsoption kann ein Blick auf Vorschläge für den Energiesektor geworfen werden, Energy rules Framework – Consultation Paper, Juli 2020, abrufbar unter: https://www.accc.gov.au/focus-areas/consumer-data-right-cdr/cdr-in-the-energy-sector/energy-rules-framework-consultation.

oder bereitgehaltenen Daten nach vertraglich vereinbarten oder gesetzlich vorgegebenen Daten-Governance-Regelungen zumindest auch im Fremdinteresse mittelt.

Neben dieser Zugangsmittelung können Datentreuhänder eine Vielzahl weiterer Funktionen übernehmen, die jedenfalls z.T. von der Datenstrategie der Bundesregierung auch adressiert werden: Anonymisierung und Pseudonymisierung, Qualitätssicherung der Datensätze und Verwaltung der Zugangsrechte. Eine weitere wichtige Aufgabe könnte es sein, dass die Datentreuhand die Zugangsentscheidung nach (gesetzlich oder privatautonom) vorgegebenen Daten-Governance-Regelungen trifft und damit eine große Hilfe für die ansonsten zugangsverpflichtete Entität sein könnte. Auch die Verarbeitung besonders sensibler Daten, z.B. aus dem Gesundheitsbereich, in einem geschützten Datentreuhandraum ist möglich. Insgesamt können Datentreuhandmodelle damit neben Datenteilungsaspekten auch in erheblichem Umfang zu einem verbesserten Datenschutz beitragen. Ein Spannungsfeld zwischen Datenzugang, Datennutzung und Datenschutz muss damit gerade nicht existieren.

Die Datenstrategie stellt darauf ab, dass für derartige Datentreuhandmodelle keine neue Bürokratie geschaffen werden sollte. Dem ist zuzustimmen und hierauf sollte auch im Data Governance Act hingewirkt werden, der nicht selbst Datenzugangsansprüche gewährt, sondern allein die infrastrukturellen Treuhandlösungen regulieren will. Insgesamt bedarf es einer ermöglichenden, anreizbasierten Regulierung, die auf einer noch vorzunehmenden Systematisierung möglicher Datentreuhandlösungen beruht und die in Abhängigkeit von bestimmten Risikoparametern entscheidet, ob überhaupt und ggf. wie viel Regulierung für das konkrete Datentreuhandmodell erforderlich ist. Wichtig ist letztlich auch, Datenzugangsrechte Daten-Governance-Erwägungen und Datentreuhandmodelle als materiell-rechtliche und infrastrukturelle

Lösung zusammen zu denken. Denn der beste Datenzugangsanspruch und die beste Daten-Governance-Lösung hilft nicht, wenn er/sie nicht im Rahmen einer bestehenden Infrastruktur geltend gemacht werden kann. Das beste Datentreuhandmodell funktioniert nicht, wenn erforderliche Datenzugangsansprüche bzw. Daten-Governance-Lösungen fehlen. Gemeinsam gedacht haben Datenzugangsansprüche und Datentreuhandmodelle dagegen das Potential, eine erhebliche Vielzahl derjenigen Probleme zu lösen, vor denen die Datenwirtschaft derzeit steht.

## III. Bestehende Rechtsunsicherheit

Neben fehlenden materiell-rechtlichen Datenzugangsansprüchen und infrastrukturellen Datentreuhandlösungen ist die v.a. aber nicht nur im Bereich des Datenschutzrechts bestehende Rechtsunsicherheit der wesentliche Faktor, der eine Datenzugangsgewährung v.a. auf freiwilliger Basis verhindert. IM Grundsatz ist dabei nicht das Datenschutzrecht selbst der Hemmschuh, sondern die Rechtsunsicherheit bei seiner Anwendung. Partielle Modifikationen des Datenschutzrechts, insbesondere der DSGVO könnten aber erheblich zur Verbesserung der Rechtssicherheit beitragen. Dies soll im Folgenden erläutert werden:

### 1. Standards zur Anonymisierung und Vermutungsregelungen

Die Datenstrategie der Bundesregierung setzt zur Verbesserung der Rechtssicherheit v.a. auf technische Lösungen und Standards zur Anonymisierung. Dies allein wird aber nicht reichen. Konkret erforderlich sind darüber hinaus gesetzliche Vermutungsregelungen dahingehend, dass bei Einhaltung der Standards eine Anonymisierung unwiderleglich vermutet wird. Denn wie auch der BfDI zutreffend feststellt, kann eine

*„valide Anonymisierung –je nach Art der zu anonymisierenden Daten und Kontext der Verarbeitung –eine Herausforderung für den jeweiligen Verantwortlichen bedeuten [...] und [es darf] nicht vorschnell von einer hinreichenden Anonymisierung ausgegangen werden [...].“*[17]

Wenn das aber der Fall ist, kann Rechtssicherheit einzig durch eine Kombination von Anonymisierungsstandards und entsprechenden Vermutungsregeln hergestellt werden.

## 2. Erlaubnistatbestand zur Erhebung von Daten zwecks Anonymisierung

Auch eine Anonymisierung der Daten erfordert es aber, die Daten zunächst nicht anonymisiert zu erheben und zu speichern, um sie anschließend dem Anonymisierungsvorgang zu unterziehen. In Bereichen wie der Erhebung von Fahrverhaltensdaten zur Produktverbesserung aber auch beim Einsatz von Smart Devices, die nun einmal einer bestimmten Person zugeordnet sind, erscheint es schwierig, wenn nicht gar ausgeschlossen, bereits die Erhebung der Daten anonymisiert durchzuführen. Da die Datenerhebung zu Zwecken der Auswertung mittels Big-Data Analysemethoden auch nur schwerlich auf einen Erlaubnistatbestand oder eine Einwilligung gestützt werden kann, ließe sich über einen Erlaubnistatbestand ähnlich § 44a UrhG zur kurzfristigen Zwischenspeicherung zwecks Anonymisierung der Daten nachdenken. Dies wäre ein wesentlicher Schritt, um gerade solche Datenverarbeitungen zu rechtfertigen, an denen Gesellschaft, Wirtschaft, Politik und Wissenschaft ein Interesse haben. Daten aus dem vernetzten Fahrzeug, Smart Devices etc. ließen sich so rechtssicher erheben, das informationelle Selbstbestimmungsrecht des Betroffenen würde aber

[17] Siehe https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 18.02.2021.

dadurch geschützt, dass die Daten automatisiert in anonymisierte Daten umgewandelt und die Ausgangsdaten anschließend gelöscht würden. Auch hier bedarf es aber ausreichender Regulierung der Anonymisierungstechnik, um die Löschung unwiederbringlich auszugestalten und das informationelle Selbstbestimmungsrecht damit ausreichend zu schützen.

Alternativ zu einem entsprechend eindeutig ausgestalteten Erlaubnistatbestand, der freilich einer Einigung auf europäischer Ebene bedürfte, könnte es sich auch anbieten, jedenfalls für die Verarbeitung nicht-sensibler Daten Leitlinien für die Abwägung im Rahmen des Art. 6 Abs. 1 lit. f DSGVO zu erlassen, die die Anwendung des Erlaubnistatbestands auf die gesamtgesellschaftlich erwünschten Datenverarbeitungen bei entsprechender Anonymisierung der Daten festschreiben. Auch auf diesem Wege ließe sich sicherlich zu mehr Rechtssicherheit beitragen, als es derzeit ohne leitende Vorgaben zur Interessenabwägung in dem hier interessierenden Bereich der Fall ist.[18]

### 3. Leitlinien zur Datenverarbeitung durch Datentreuhänder

Erforderlich sind weiterhin Leitlinien zur Datenverarbeitung durch Datentreuhänder gem. Art. 6 Abs. 1 lit. f DS-GVO und ggf. Modifikationen in den hohen Voraussetzungen der Einwilligung zwecks Verarbeitung von Daten in Datentreuhandlösungen. Wird sichergestellt, dass es sich um vertrauensvolle Datentreuhandlösungen handelt, wird das informationelle Selbstbestimmungsrecht bei der Verarbeitung in diesen geschützten Datenräumen nicht in gleicher Weise gefährdet wie im Falle der Verarbeitung durch andere Dritte, sodass es möglich wäre, die die Voraussetzungen der Datenverarbeitung durch Datentreuhänder zu senken.

### 4. Umgang mit Mixed Data Sets

[18] Die Ausführungen unter 2. entsprechen den Ausführungen der Verfasserin in GRUR Int. 2017, 1040, 1047.

Eine Erweiterung des Datenschutzrahmens im Hinblick auf sogenannte Mixed Data Sets, die immer auch personenbezogene Daten beinhalten, ist nicht erforderlich, da derartige Datensets ohnehin nach den Vorgaben des Datenschutzrechts zu behandeln sind. Die Einführung einer Positivliste plastischer Regelbeispiele für nicht-personenbezogene Daten scheint dagegen nicht ratsam, da Daten je nach Kontext als personenbezogen oder nicht personenbezogen zu qualifizieren sind und dies auf einem Urteil des EuGH beruht.[19] Hier valide Aussagen im Sinne einer Positivliste zu treffen, auf die sich der Rechtsanwender verlassen kann, scheint daher kaum möglich. Sinnvoller scheinen die o.g. Vermutungsregelungen bei Einhaltung vorgegebener Anonymisierungsstandards in Kombination mit einem Erlaubnistatbestand zur Erhebung personenbezogener Daten zwecks Anonymisierung entsprechend § 44a UrhG.

## 5. Stellvertretungslösungen für die Erklärung und den Widerruf der datenschutzrechtlichen Einwilligung

Sollen effiziente PIMS-Modelle ermöglicht werden, bedarf es v.a. einer Stellvertretungslösung für die Erklärung und den Widerruf von Einwilligungen und die Ausübung von Betroffenenrechten. Beides ist unter der DS-GVO derzeit streitig.[20] Richtigerweise muss aber eine Stellvertretung sowohl bei der Erklärung und beim Widerruf datenschutzrechtlicher Einwilligungen als auch bei der Ausübung von Betroffenenrechten möglich sein, denn auch die Entscheidung für

[19] EuGH, Urt. v. 19.10.2016 – C-582/14, ECLI:EU:2016:799 = NJW 2016, 3579 – *Breyer/Deutschland*.

[20] Vgl. etwa *Ernst*, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, S. 110-114, 111; Simitis/Hornung/Spiecker-*Klement*, Art. 7 DSGVO Rn. 37; Taeger/Gabel-*Taeger*, Art. 7 DSGVO Rn. 10; Gola-*Schulz*, Art. 7 DSGVO Rn. 9; Ehmann/Selmayr-*Heckmann/Paschke*, Art. 7 DSGVO Rn. 34; Hoeren/Sieber/Holznagel-*Helfrich*, Teil 16.1.D.I. Rn. 51; Specht/Mantz-*Specht*, § 9 Rn. 42; Sydow-*Ingold*, Art. 7 DSGVO Rn. 19; Kühling/Buchner-*Buchner/Kühling*, Art. 7 DSGVO Rn. 31; *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, im Erscheinen.

eine solche Stellvertretungslösung ist letztlich Ausübung des Rechts auf informationelle Selbstbestimmung.[21]

Geht man – mit gewichtigen Stimmen in der Literatur[22] – davon aus, dass die Einwilligung auch in Stellvertretung erteilt werden kann, dann sind an die Vollmachtserteilung aber jedenfalls dieselben Anforderungen zu stellen wie an die Einwilligung selbst.[23] Dies widerspricht zwar § 167 Abs. 2 BGB, die Einwilligung nach der DSGVO ist aber auch nicht nach den Maßstäben des nationalen Rechts, sondern unionsrechtskonform auszulegen. Die hohen Voraussetzungen der Einwilligung, die eine echte Selbstbestimmung des Betroffenen gewährleisten sollen, würden unterlaufen, wenn die Voraussetzungen nicht auch für die Vollmachtserteilung gelten würden. Das bedeutet zivilrechtlich, dass lediglich eine Spezialhandlungsvollmacht statt einer Generalhandlungsvollmacht erteilt werden kann.

Ebenso ist die Übermittlung der Einwilligung des Betroffenen durch den Datentreuhänder als Erklärungsbote möglich[24] und dies jedenfalls im Wege eines Erst-Recht Schlusses: Ist sogar die Stellvertretung zulässig, so muss jedenfalls die weniger eingriffsintensive Botenschaft rechtlich möglich sein. Viele PIMS werden derzeit wohl – wenn überhaupt - allein auf Grundlage einer Botenschaft tätig,

[21] Specht/Mantz-*Specht*, § 9 Rn. 42; Sydow-*Ingold*, Art. 7 DSGVO Rn. 19; Kühling/Buchner-*Buchner/Kühling*, Art. 7 DSGVO Rn. 31; *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, im Erscheinen.

Sydow-*Ingold*, Art. 7 DSGVO Rn. 19; Kühling/Buchner-*Buchner/Kühling*, Art. 7 DSGVO Rn. 31; *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, im Erscheinen.

[23] So zutreffend *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, im Erscheinen.

[24] *Lüdemann/Pokrant*, Die Einwilligung beim Smart Metering, DuD 2019, S. 365-370, 368; *Hoffmann*, Einwilligung der betroffenen Person als Legitimationsgrundlage eines datenverarbeitenden Vorgangs im Sozialrecht nach dem Inkrafttreten der DSGVO, NZS 2017, S. 807-812, 808; *Ernst*, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, S. 110-114, 111; Taeger/Gabel-*Taeger*, Art. 7 DSGVO Rn. 9; Wolff/Brink-*Stemmer*, Art. 7 DSGVO Rn. 31; Sydow-*Ingold*, Art. 7 DSGVO Rn. 20; Kühling/Buchner-*Buchner/Kühling*, Art. 7 DSGVO Rn. 31; Simitis/Hornung/Spiecker-*Klement*, Art. 7 DSGVO Rn. 37.

weil ihnen der eigene Entscheidungsspielraum fehlt. Effizient und hilfreich scheint aber erst ein Modell, indem eben nicht diese Botenschaft, sondern eine Stellvertretungslösung gewählt würde, weil die PIMS nur dann einen eigenen Entscheidungsspielraum im Interesse des Betroffenen ausüben können.

Zu Zwecken der Rechtssicherheit wäre eine gesetzliche Normierung der Stellvertretungsmöglichkeit sowie der Botenschaft im Rahmen der Einwilligung sinnvoll, jedenfalls Leitlinien durch DSK oder europäischen Datenschutzbeauftragten sollten aber erfolgen. Die erst Anfang Mai 2020 aktualisierten Guidelines zur Einwilligung[25] ließen sich beispielsweise ergänzen, ebenso die Stellungnahme des Europäischen Datenschutzbeauftragten zu PIMS.[26]

## 6. Stellvertretungslösungen zur Ausübung von Betroffenenrechten

Zugunsten des Betroffenen würde es sich ebenfalls auswirken, wenn Datentreuhandlösungen, z.B. in Form von PIMS die Betroffenenrechte gemäß Art. 13 ff. DSGVO geltend machen und Einwilligungen widerrufen könnten. Die Einbindung eines Datentreuhänders ist zur Geltendmachung der Betroffenenrechte in der DSGVO aber nicht explizit vorgesehen. Die EU-Kommission geht in ihrem Entwurf eines Data Governance Act in Erwägungsgrund 24 sogar explizit davon aus, dass Betroffenenrechte nur von der betroffenen Person selbst ausgeübt und nicht an einen Dritten delegiert oder übertragen werden können. Der DSGVO ist die Geltendmachung der Betroffenenrechte durch Dritte aber durchaus jedenfalls für die in Art. 77, 78, 79 und Art. 82DSGVO genannten Rechte bekannt, vgl. Art. 80 Abs. 1 DSGVO. Insofern stellt sich die Frage, ob dies nicht auch

[25] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4.5.2020, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[26] Europäischer Datenschutzbeauftragter, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), Stellungnahme 9/2016, S. 6, abrufbar unter : https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf, zuletzt abgerufen am 18.02.2021.

mit Blick auf die Betroffenenrechte bereits de lege lata der Fall sein muss oder jedenfalls de lege ferenda im Betroffeneninteresse vorgesehen werden sollte.

Teleologisch wäre es auch hier 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 nach Art. 80 DSGVO zulassen sollte, 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 nicht begründbar. Richtigerweise wird daher vertreten, dass auf Grundlage des Art. 80 Abs. 1 DSGVO auch Ansprüche auf Information, Auskunft und Unterlassung gegen Verantwortliche und Auftragsverarbeiter für die betroffene Person geltend gemacht werden können.[27] Mit diesen Rechten sollte es aber nicht sein Bewenden haben. Mit der dargelegten teleologischen Argumentation eines primär verfolgten Betroffenenschutzes sollte Art. 80 Abs. 1 DSGVO vielmehr auf sämtliche Betroffenenrechte der Art. 15 ff. DSGVO Anwendung finden. Gleichwohl gilt auch im europäischen Recht: Der Wortlaut ist die Grenze der Auslegung, weshalb eine Ausweitung von Art. 80 DSGVO im Wege des Analogieschlusses a minori ad maius auf die für den Betroffenen so elementar wichtigen Betroffenenrechte erfolgen müsste. Die Rechtsfortbildung mittels Analogie ist auch im Unionsrecht methodisch anerkannt.[28] Wünschenswert wäre es aber, dass der Gesetzgeber die Ausübung der Betroffenenrechte durch dritte Personen explizit normiert, um Rechtsunsicherheit vorzubeugen bzw. zu beseitigen.

[27] Kühling/Buchner-*Bergt*, Art. 80 DSGVO Rn. 11; *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, im Erscheinen.

[28] *Schneider*, Kollision von Controllership und One-Stop-Shop, ZD 2020, S. 179-184, 183 m.w.N.

### 7. AGB-Kontrolle von Einwilligungserklärungen

Statt eines strengen Koppelungsverbotes bedarf es spezifischer Normen zur Klauselkontrolle vorformulierter Einwilligungen, die im Rahmen von Vertragsverhältnissen erklärt werden. Denn wird eine Einwilligung im Rahmen eines Vertragsverhältnisses erklärt, so erfolgt sie in Ausübung einer privatautonomen Entscheidung. Das Koppelungsverbot ist dann nicht der richtige Kontrollmaßstab, sondern die §§ 134, 138 BGB sowie die Klauselkontrolle.

### 8. Datenbankschutz im Urheberrecht

Nicht nur die Anwendung des Datenschutzrechts aber führt zu Rechtsunsicherheit. Auch der Datenbankschutz im Urheberrecht und mögliche weitere Schutzrechte an (personenbezogenen und nicht-personenbezogenen) Daten können zu derartiger Rechtsunsicherheit beitragen. Bei der Etablierung eines Rechtsrahmens für Datenzugangsansprüche ist daher über das Zusammenspiel der betroffenen Rechtsgebiete zu entscheiden. Bei der Überarbeitung der Datenbankrichtlinie im Urheberrecht sollte daher z.B. ebenfalls über erforderliche Datenzugangsansprüche im o.g. Sinne nachgedacht werden.