FAIR Newsletter

Ausgabe 08

Juni 2022

Newsletter zu aktuellen rechtlichen Entwicklungen rund um das Projekt FAIR Data Spaces

FAIR Data Spaces

WWU MÜNSTER

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

Förderkennzeichen FAIRDS

Liebe Leserinnen und Leser,

wie jeden Monat folgt eine Zusammenschau spannender Rechtsprechung und Literatur zu Rechtsfragen rund um immaterialgüter- und datenschutzrechtliche Rechtsfragen aus dem Projekt FAIR Data Spaces.

In dieser Ausgabe berichten wir unter anderem über die Stellungnahme des NFDI zum EU Data Act v. 13.05.2022. Darauf folgt ein Urteil des EuGH vom 21.06.2022, in welchem er entschieden hat, dass das Verarbeiten von Fluggastdaten nach der PNR-Richtlinie auf das absolut Notwendige beschränkt werden muss. Schließlich folgen drei aktuelle Aufsätze über staatliche Steuerungsmöglichkeiten zur Förderung des Teilens von Forschungsdaten, über den Entwurf des Daten-Governance-Gesetzes und über die Bedeutung sowie den Umfang des Forschungsdatenzugangs.

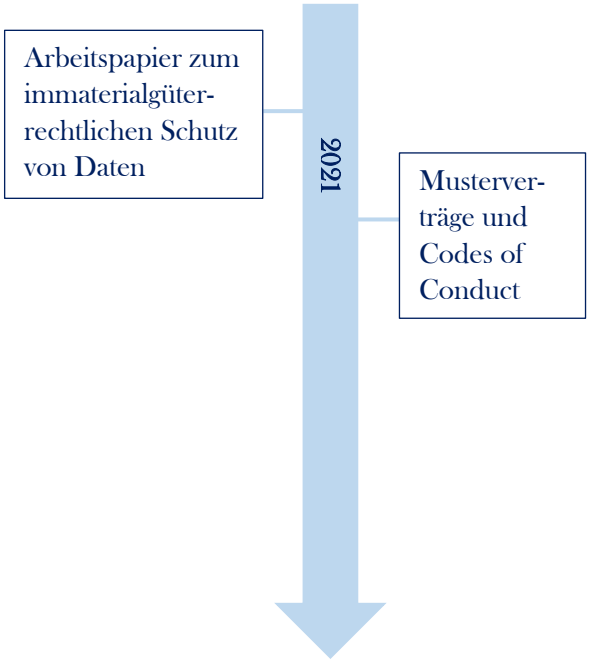
Treten Sie bei Fragen und Anregungen gerne mit uns in Kontakt (ITM Universität Münster, Leonardo Campus 9, D-48149 Münster, Projekt FAIR Data Spaces julian.grosse-ophoff@uni-muenster.de).

Weitere Informationen zum Projekt **FAIR Data Spaces** erhalten Sie unter https://www.itm.nrw/fair-data-spaces/.

Viel Spaß beim Lesen wünscht Ihr **münsteraner FAIR Team!**

Julian Große-Ophoff, Hendrik Risthaus & Max Husmann

Roadmap – Wo stehen wir?



I.

1. Update Fair Data Spaces: Stellungnahme des NFDI zum EU Data Act v. 13.05.2022

Die NFDI-Sektion ELSA (Ethic, Legal and Social Aspects) hat sich in einer Stellungnahme vom 13.05.2022 als erste NFDI-Sektion zu dem Gesetzesentwurf zum EU Data Act geäußert. Die Stellungnahme bezieht sich im Wesentlichen (nur) auf den durch den EU Data Act intendierten erleichterten Zugang für öffentliche Stellen und Forschungseinrichtungen zu Daten aus wissenschaftliche Zwecken. Grundsätzlich begrüßt ELSA den Gesetzentwurf, sieht aber bezüglich einiger Aspekte noch Klärungsbedarf.

So sieht ELSA etwa bezüglich der **Abgrenzung zwischen EU Data Act (DA) und EU Data Governance Act (DGA)** Klärungsbedarf. Das Verhältnis des DA und des DGA sei z.B. in Bezug auf die Verarbeitung von personenbezogenen Daten nicht eindeutig (siehe die Vorgaben zum Profiling nach Art. 6 lit. b) DA im Kontext des Art. 18 Abs. 5 DA). Zudem würden sich DA und DGA in der aktuellen Entwurfsfassung bei der Datenweitergabe im B2G Kontext überschneiden. Nach dem DA muss die datenerhaltende Institution zu Non-Profit-Zwecken, ohne eigenes Gewinninteresse, handeln (Art. 21 Abs. 2 DA). Die Intention des Art. 21 DA zeige somit Parallelen zum Modell des Datenaltruismus des Art. 15 DGA auf: Auch hier handelt es sich bei der datenerhaltenden Stelle um eine Non-Profit-Organisation (Art. 16 DGA), die die Daten nicht für eigene Zwecke nutzen darf (Art. 16 lit. c) DGA). Dabei ist das Modell hauptsächlich zur Unterstützung der Forschung, insbesondere Statistikzwecken, gedacht (EW 39 DGA). Zwar sei der Ursprung der Daten unterschiedlich (Daten nach Art. 21 DA entstammen Datensätzen öffentlicher Stellen, Art. 15 DGA beruht auf einer Einwilligung), es könne aber zu dennoch zu Überschneidungen im Anwendungsbereich kommen. Diese „Zweigleisigkeit" könne zu Rechtsunsicherheit führen.

Weiterhin sei die Definition von „exceptional need" (Art. 15 DA, Voraussetzung für ein Datenzugangsrecht nach Art. 14 Abs. 1 DA) intransparent und, indem sie auf eine „exceptional situation" abstelle, unzeitgemäß. Bei vielen heutigen Gefahren, wie etwa dem Klimawandel oder Finanzkrisen, handele es sich um anhaltende Krisen und eben nicht um „außergewöhnliche" Situationen. Der Mehrwert insbesondere nicht personenbezogener Daten bestehe jedoch regelmäßig gerade in deren Potenzial, sie durch wissenschaftliche Methoden in handlungsleitend Erkenntnisse und Wissen umzuwandeln. Hierbei handele es sich allerdings um einen langwierigen Prozess. **Es bedürfe eines kontinuierlichen Datenzugangs zur Gefahrenabwehr**. Im Falle der Notwendigkeit eines kurzfristigen Datenzugangsrecht zur Gefahrenabwehr sei ohnehin das allgemeine nationale Polizei- und Gefahrenabwehrrecht vorrangig (Art. 1 Abs. 4 DA).

Unklarheiten gebe es zudem **im Zusammenhang mit der Möglichkeit der Datenteilung öffentlicher Stellen mit Forschungseinrichtungen (Art. 21 DA)**. Da auch Forschungseinrichtungen öffentliche Stellen seien können (EW 56 DA), bedürfe es klarerer Definitionen und Abgrenzungen.

Schließlich enthält der DA eine Zweckbindung der Daten. Sie dürfen für keinen anderen Zweck als in der Einwilligung angegeben genutzt werden (Art. 19 Abs. 1 lit. a) DA). Diese Zweckbindung gilt auch für die Datenweitergabe von öffentlichen Stellen an Forschungseinrichtungen (Art. 21 Abs. 1 und 3

DA). Es sei **unklar, inwiefern wissenschaftliche Publikationen mit dem ursprünglichen Zweck vereinbar** seien. Daher sei eine klarstellende Regelung wie in Art. 5 Abs. 1 lit. b) DSGVO zugunsten der wissenschaftlichen Forschung im Sinne einer höheren Rechtssicherheit wünschenswert.

Die Stellungnahme ist 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/F3258672_en

2. Evaluation zum Schutz maschinengenerierter Daten

Die Bedeutung maschinengenerierter Rohdaten – d.h. "maschinenlesbar codierte Informationen, die von einer Datenverarbeitungsanlage automatisch erzeugt und verarbeitet werden" ist nicht nur für unsere Informationsgesellschaft im Allgemeinen, sondern auch für das FAIR Data Spaces im Speziellen von wachsender Bedeutung. So sammeln und generieren etwa intelligente Fahrzeuge zunehmend autonom Daten. Diese Datensätze bilden so dann die erste Stufe einer späteren Wertschöpfungskette und sind daher von erheblichen Wert für die Industrie und Forschung. Welche potentiellen Probleme maschinengenerierte Rohdaten in Bezug auf den immaterialgüterrechtlichen Schutz mitsichbringen, soll nachfolgend anhand des Urheber- und Geschäftsgeheimnisrechts skizziert werden.

a) Eingeschränkter urheberrechtlicher Schutz

Im Ausgangspunkt setzt der urheberrechtliche Schutz gem. § 2 Abs. 2 UrhG eine persönliche geistige Schöpfung voraus. Wie bereits der Wortlaut nahelegt, sind persönliche Schöpfungen nur solche Werke, die ein Mensch geschaffen hat. Urheber kann folglich keine Maschine sein, sondern lediglich natürliche Personen. Bei maschinengenerierten Daten fehlt es gerade an einer derartigen menschlichen Schöpfung. Natürlich darf sich zur Herstellung des Werkes auch technischen Hilfsmitteln bedient werden. Sofern der Erzeugung allerdings ein weitgehend autonom arbeitender Algorithmus zugrunde liegt – wie dies bei maschinengenerierten Daten zumeist der Fall ist – können diese nicht mehr dem Schöpfer des zugrundeliegenden Computerprogramms zugerechnet werden. Ebenso scheitert ein urheberrechtlicher Schutz als Computerprogramm (§§ 69a ff. UrhG) aus, da vielmehr das Resultat eines Computerprogramms sind. Darüber hinaus können maschinengenerierte Daten grundsätzlich zwar Teil einer Datenbank sein, welche wiederum den auf Investitionsschutz ausgerichteten Rechten des Datenbankherstellers (§§ 87a ff. UrhG) unterfällt. Diese sui-generis-Rechte schützen allerdings nicht die einzelnen in der Datenbank enthaltenen Daten, sondern lediglich die Datenbank als strukturelle Gesamtheit.

b) Potentieller Schutz nach dem Geschäftsgeheimnisrecht

Der Schutz von Geschäftsgeheimnissen wurde in der jüngeren Vergangenheit durch die RL (EU) 2016/943 harmonisiert. Die Umsetzung dieser Richtlinie erfolgte in Deutschland durch die Verabschiedung des Geschäftsgeheimnisgesetzes (GeschGehG). Eine wesentliche Neuerung zu dem bisherigen Geheimnisschutz ist die Einführung einer Legaldefinition des Begriffes „Geschäftsgeheimnis". Gem. § 2 Nr. 1 GeschGehG sind darunter Informationen zu verstehen, die (a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher

von wirtschaftlichem Wert ist und (b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und (c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht". Hinsichtlich des Schutzes maschinengenerierter Daten stellt sich nun die Fragen, ob auch solche Datensätze geschützt werden, die im Grunde von jedermann erhoben werden könnten. Beispielhaft sind geologische Daten bereits in der Umwelt vorhanden. Sie werden durch die sensorgestützte Erhebung lediglich „sichtbar" gemacht. Es vermag schwer fallen derartige Daten als noch als „geheim" zu bezeichnen. Ausschlaggebend ist jedenfalls, ob die besondere Zusammensetzung der Datensätze Geheimnischarakter aufweist. Dies könnte etwa dann der Fall sein, wenn die Aggregation unter erheblichen zeitlichen und finanziellen Aufwand stattfand. Dies kann jedoch lediglich anhand einer einzellfalgerechten Prüfung erfolgen.

Herzstück des Geschäftsgeheimnisrechts sind jedoch die angemessenen Maßnahmen zur Geheimhaltung der jeweiligen Informationen. Sie stellen auch den wesentlichen Unterschied zum bisherigen Geheimnisrecht dar, wonach es lediglich auf einen erkennbaren Geheimhaltungswillen ankam. Es wird für Schutz von maschinengenerierten Daten in den FAIR Data Spaces daher erforderlich sein, dass zum einen die beteiligten Institutionen und Unternehmen intern organisatorisch- personelle Maßnahmen zur Geheimhaltung treffen und zum anderen während des Datenaustausches mit Dritten verbindliche Absprachen schließen, die entsprechende Geheimhaltungspflichten für beide Vertragspartner beinhalten.

3. Resümee

Der immaterialgüterrechtliche Schutz maschinengenerierter Daten ist auch in den FAIR Data Spaces allgegenwärtig. Schlussendlich ist er vor allem eine Frage des Einzelfalls, die eine genaue juristische Analyse unabdingbar macht. Er ist aber auch davon abhängig, dass rechtssichere Abreden zum Datenaustausch in den FAIR Data Spaces geschlossen werden. Dabei wird das ITM Münster unterstützend mitwirken, indem wir bestehende Verträge auf potentielle Haftungslücken überprüfen oder Musterverträge bzw. Codes of Conduct an die Hand geben.

II.

Aktuelle Rechtsprechung

1. Urteil des EuGH, Urt. v. 21.06.2022 - Az.: C-817/19

Der EuGH hat entschieden, dass das Verarbeiten von Fluggastdaten nach der PNR-Richtlinie auf das absolut Notwendige beschränkt werden muss. Besteht **keine reale und aktuelle oder vorhersehbare terroristische Bedrohung**, so stellt die **Verarbeitung von Fluggastdaten ein Verstoß gegen das Unionsrecht** dar.

Die PNR-Richtlinie sieht die systematische Verarbeitung von PNR-Daten (Passager Name Record) zur Bekämpfung von Terrorismus und schwerer Kriminalität vor. Sie gilt für Flüge zwischen der Union und Drittstaaten, kann von den Mitgliedstaaten gem. Art. 2 PNR-Richtlinie auch auf Flüge innerhalb der Union angewandt werden. Der gemeinnützige Verein Ligue des droits humains hat gegen das belgische Gesetz zur Umsetzung der Richtlinie im Juli 2017 eine Nichtigkeitsklage vor dem begischen Verfassungsgerichtshof erhoben. Das belgische Gesetz verletze das unionsrechtlich garantierte Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten. Problematisch sei zudem der große Umfang der PNR-Daten sowie der allgemeine Charakter ihrer Erhebung, Übermittlung und Verarbeitung. Weiterhin schränke das belgische Gesetz die Freizügigkeit ein.

Der EuGH stellt fest, dass es durch die PNR-Richtlinie zu schwerwiegenden Eingriffen in Art 7 (Achtung des Privat- und Familienlebens) und 8 (Schutz personenbezogener Daten) der Charta kommt, insbesondere soweit die Richtlinie auf die Schaffung eines Systems kontinuierlicher, nicht zielgerichteter und systematischer Überwachung abzielt, dass die automatisierte Überprüfung personenbezogener Daten sämtlicher Personen einschließt, die Flugreisen unternehmen. Entscheidend für die mögliche Rechtfertigung durch die Mitgliedstaaten ist die zu bestimmende Schwere des Eingriffs und inwiefern diese in einem angemessenen Verhältnis zum Gemeinwohl stehen. Die in der Richtlinie vorgesehenen Befugnisse sind eng auszulegen, und **auf das für die Bekämpfung terroristischer Straftaten und schwerer Kriminalität absolut Notwendige zu beschränken**. Zudem muss die Anwendung des durch die Richtlinie geschaffenen Systems auf terroristische Straftaten und auf schwere Kriminalität mit einem - zumindest mittelbaren - objektiven Zusammenhang mit der Beförderung von Fluggästen beschränkt werden. Mit der Beschränkung auf das absolut Notwendige sind mehrere Voraussetzungen verknüpft. Unter anderem werden die Grenzen des absolut Notwendigem nur in einer Situation nicht überschritten, in der es hinreichend konkrete Umstände für die Annahme gibt, dass der Mitgliedstaat mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist.

Bei der Vorabüberprüfung anhand im Voraus festgelegter (objektiver) Kriterien dürfen zudem keine Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme („machine learning') herangezogen werden, soweit diese - ohne menschliche Einwirkung und Kontrolle - den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern könnten. Außerdem müsse bei der Vorabüberprüfung das Diskriminierungsverbot beachtet werden.

Eine nachträgliche Zurverfügungstellung zum Zwecke der nachträglichen Überprüfung der PNR-Daten nach Ankunft oder dem Abflug der betreffenden Person dürfe grundsätzlich – außer in hinreichend begründeten Eilfällen – nur nach einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle erfolgen.

Bezüglich der Speicherfrist von PNR-Daten stellt der EuGH fest, dass Art. 12 der PNR-Richtlinie im Licht der Art. 7 und 8 sowie von Art. 52 Abs. 1 der Charta nationalen Rechtsvorschriften entgegensteht, die eine allgemeine, unterschiedslos für alle Fluggäste geltende Speicherfrist dieser Daten von fünf Jahren vorsehen.

Das Urteil ist abrufbar unter:

https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

III.

Aktuelle Literatur

1. Overkamp/Tormin: Staatliche Steuerungsmöglichkeiten zur Förderung des Teilens von Forschungsdaten, in: OdW 2022.

In ihrem Aufsatz erläutern Philipp Overkamp und Miriam Tormin die rechtlichen Rahmenbedingungen sowie verschiedene Möglichkeiten der direkten und indirekten staatlichen Steuerung zur Förderung des Teilens von Forschungsdaten.

Das Data-Sharing sei von **überragender Bedeutung**, um die Gewinnung neuer Erkenntnisse in der Forschung zu beschleunigen. Nicht zuletzt habe dies die Impfstoffentwicklung im Rahmen der SARS-CoV-2-Pandemie gezeugt. Damit Deutschland „wettbewerbsfähig" bleibe, müsse das Data-Sharing auch hier zulande ausgeschöpft werden.

Damit keine geschönten Datensätze entstehen, sollten **möglichst alle potentiell relevanten Daten** offengelegt werden.

Der aus dem Förderauftrag der Wissenschaftsfreiheit erwachsende Informationszugangsanspruch gebiete dabei zumindest einen **Zugang für jene, die ein wissenschaftliches Nutzungsinteresse plausibilisieren** können.

Ob der Staat das Teilen von Forschungsdaten fördern darf, oder sogar muss, sei mangels determinierter juristischer Vorgaben eine politische Entscheidung.

Hinsichtlich des „**Wie´s**" stehen dem Staat verschiedene Steuerungsmodi zur Verfügung. Denkbar seien eine **direkte und eine indirekte Steuerung**. Die indirekte Steuerung, die Anreize zur Offenlegung der Daten schaffte, ohne entgegengesetztes Verhalten zu verbieten, sei angesichts der hohen **grundrechtlichen Eingriffsintensität der direkten Steuerung** als unmittelbar und imperativ geltender Verhaltensbefehl, wahrscheinlicher.

Verpflichtete man Wissenschaftler pauschal, alle im Rahmen eines Forschungsprojektes erhobenen Rohdaten mit der Öffentlichkeit zu teilen, läge ein **Eingriff** in die von **Art. 5 III 1 GG** geschützte negative Publikationsfreiheit und in die allgemeine Wissenschaftsfreiheit der Forscher vor. Zwar läge in der objektiv-rechtlichen Komponente der Wissenschaftsfreiheit, welche vom Staat die Schaffung von Rahmenbedingungen zur Ermöglichung einer innovativen Forschung verlange, ein **legitimer Zweck**. Eine pauschale Pflicht zur Datenoffenlegung wäre aber trotzdem nicht mit der Verfassung in Einklang zu bringen, da die Funktionalität des Wissenschaftsbetriebes nicht an sich gefährdet sei.

Dementsprechend sei auf eine **indirekte Steuerung** der Förderung des Data-Sharings zu verweisen:

Eine solche könne darin bestehen, Förderorganisationen und Forschungseinrichtungen aufzutragen, über die Vorteile von Data-Sharing **aufzuklären** und **Empfehlungen** auszusprechen. Grundrechtlich bedenklich wäre es, wenn damit eine Herabsetzung jedes Adressaten einherginge, der der Empfehlung nicht nachkommt.

Eine weitere Möglichkeit bestünde darin, die Adressaten mit der zu erwartenden **öffentlichen Anerkennung** im Falle der Nennung der Datenerheber zu motivieren. Ebenfalls könnten **Auszeichnungen und Ehrentitel** für besonderes Open-Science-Engagement verliehen werden.

Um diejenigen Wissenschaftler zu privilegieren, die zum Teilen von Daten bereit sind,

könnten **„Open-Science-Datenbanken“** bereitgestellt werden, die Forschungsdaten speichern und nur denjenigen den Zugang gewähren, die selbst offen mit ihren Daten umgehen. Dadurch entstünden allerdings ein Sanktionscharakter und eine Diskriminierung, die mit Art. 5 III GG nicht zu vereinen wären. Weniger eingreifend wäre es, jedem den Zugang zu der Datenbank zu gewähren, aber den Wissenschaftlern, die ihre Daten offenlegen, Extradienste anzubieten.

Eine ebenfalls indirekte Steuerung bestünde darin, das **Eiverständnis** zum Data-Sharing **als Bedingung in einen Förderantrag** aufzunehmen, welches nur mit besonderer Begründung abgelehnt werden könnte. Um dem Begründungsaufwand zu entgehen und aufgrund sozialen Drucks würden viele ihr Einverständnis erteilen.

Schließlich könnte das Data-Sharing auch als **Entscheidungskriterium bei er Fördermittelvergabe** dienen. Da Forschungsfördermittel begrenzt sind, liege grundsätzlich zumindest noch keine Diskriminierung darin, das Kriterium als eines unter vielen heranzuziehen.

Der Aufsatz ist (kostenlos) abrufbar unter:

https://intr2dok.vifa-recht.de/receive/mir_mods_00011581

2. Schildbach: Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes, in: ZD 2022.

Roman Schildbach prüft zwei der im Entwurf des europäischen Daten-Governance-Gesetzes (DGG-E) vorgesehenen Maßnahmen und deren Mehrwert v.a. hinsichtlich des zu erwartenden Zusammenspiels mit dem bisherigen datenschutzrechtlichen Regelungsgefüge.

Der DGG-E sieht zum einen die Wiederverwendung von Daten öffentlicher Stellen und zum anderen einen „Datenaltruismus“ vor.

Die **Wiederverwendung von Daten öffentlicher Stellen** für nicht-staatliche Zwecke solle **Kapitel II des DGG-E** ermöglichen, um auch der Gesellschaft zugute zu kommen. Eine Pflicht zur Datenbereitstellung statuiere der DGG-E hingegen nicht. Das „Ob“ und weitgehend auch das „Wie“ bleibe größtenteils den Mitgliedstaaten überlassen. Lediglich Ausschließlichkeitsvereinbarungen seien verboten (Art. 4 DGG-E). Zudem sehe Art. 8 DGG-E vor, dass die Mitgliedstaaten eine zentrale Informationsstelle schaffen müssen, bei der Anträge auf Datenzugang gestellt werden können und die diese Anträge dann an die entscheidenden Stellen weiterleitet. Um Anreize zur vermehrten Wahrnehmung des Datenzugangs zu schaffen, solle so in jedem Mitgliedstaat ein One-Stop-Shop-Prinzip etabliert werden. Diese Regelung stelle den **einzigen regelungstechnischen Mehrwert** dar. Ansonsten ändere sich in den Mitgliedstaaten nicht viel, denn unter den Voraussetzungen der DS-GVO war die Herausgabe von Daten der öffentlichen Hand zuvor schon möglich. Mit komplexen und langwierigen Verfahren müssen die potenziellen Datennutzer jedoch weiterhin rechnen. Schildbachs Fazit bezüglich des **harmonisierenden Effekts** der Verordnung fällt ebenfalls **ernüchternd** aus, denn er weist darauf hin, dass bisher untätige Mitgliedstaaten im besten Fall zwar zur Schaffung neuer

Datenzugangsregeln angeregt, aber nicht verpflichtet werden.

Der **Datenaltruismus (Kapitel IV DGG-E)** solle Datenspenden erleichtern. Die Art. 15 bis 17 DGG-E enthalten Regelungen zur freiwilligen Zertifizierung von Organisationen als „anerkannte datenaltruistische Organisationen". Hauptanforderungen seien die rechtliche Unabhängigkeit und „Non-Profit"-Eigenschaft. Die Kommission erhoffe sich, mittels dieser Organisation Datenarchive aufbauen zu können, welche der Allgemeinheit dienen. Mit der Zertifizierung als datenaltruistische Organisation gehe keine materiell-rechtliche Privilegierung einher. Über den Ablauf der Datenspende treffe der DGG-E so gut wie keine eigenständige Regelung und auf Grundlage der Einwilligung nach der DS-GVO sei eine Spende personenbezogener Daten auch ohne zertifizierte datenaltruistische Organisation möglich. Art. 22 DGG-E, der eine unionsweit verwendete Mustereinwilligung vorsieht, biete ebenfalls keinen Mehrwert, denn sie könne nicht wirklich mehr Rechtssicherheit bei der Frage der Genauigkeit der Zweckbestimmung schaffen. Mangels materiell-rechtlicher Regelungen verpuffe die Zertifizierung damit zu einer reinen Marketingmaße – aufgrund der zusätzlichen Bürokratie (Art. 18, 19 DGG-E) sei das Modell sogar geradezu unattraktiv.

Schlussendlich bezweifelt Schildbach, ob mehr Recht hier überhaupt zu besserem Recht führt. Er fordert den Gesetzgeber auf, entweder mehr Harmonisierung zu wagen, oder auf die Einführung der untersuchten Regelungen der DGG-E zu verzichten.

Der Aufsatz ist (im Rahmen eines beck-online Abos) abrufbar unter:

https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2022%2Fcont%2Fzd.2022.2.148.1.htm&pos=1&hlwords=on&lasthit=True

3. Specht-Riemschneider/Wehde: Forschungsdatenzugang, in: ZGI 2022.

Louisa Specht-Riemschneider und Alexander Wehde diskutieren in ihrem Aufsatz die Wichtigkeit des Forschungsdatenzugangs, dessen Art und Umfang sowie Schrankenbestimmungen de lege lata und de lege ferenda.

Der Zugang zu Daten sei für die Forschung essenziell und daher im gesamtgesellschaftlichen Interesse. Zeitgleich werde **fehlender Forschungsdatenzugang zunehmend beklagt.** Materiell-rechtliche Datenzugangsansprüche welche nicht vorrangig Wissenschaftlern zustehen - seien es vertragliche Auskunftsansprüche, datenschutzrechliche oder kartellrechtliche - werden in der Untersuchung vernachlässigt. Explizite Forschungsklauseln wie etwa in § 5a NetzDG gibt es bisher selten.

Sollten Datenzugangsansprüche auf europäischer oder nationaler Ebene eingeführt werden, müssten jeweils die Rechtspositionen des Datenzugangsadressaten, die (Unions-)Grundrechte Drittbetroffener sowie die (unions-)grundrechtlichen Interessen der Zugangssuchenden in einen angemessenen Ausgleich gebracht werden. So seien etwa der (unions-)grundrechtlich verankerte Geschäftsgeheimnisschutz, der Schutz des Geistigen Eigentums, der Schutz der Berufsfreiheit sowie andererseits auch die Gewährleistung der Forschung als legitimer Zweck und die Forschungsfreiheit zu beücksichtigen.

Auch der datenschutzrechtliche Rahmen des Forschungsdatenzugangs wird diskutiert. Specht-Riemschneider und Wehde fordern in Rahmen wissenschaftlicher Forschung weniger strenge Anforderungen an die Bestimmtheit der Einwilligung zur

Weitergabe nicht-sensibler personenbezogener Daten nach Art. 6 Abs. 1 S. 1 lit. a DS-GVO. Bei der Erhebung von Daten könne das spätere Forschungsvorhaben häufig noch nicht konkret abgesehen werden. Die Sekundärnutzung von Daten müsse zwingend auf eine Einwilligung gestützt werden. Sie ließe sich insbesondere auf Art. 6 Abs. 1 S. 1 lit. e und f DSGVO stützen.

Neben diesen (unions-)grundrechtlichen Rahmenbedingungen müsse der Forschungsdatenzugang einigen bestimmten Prinzipien folgen. Er **dürfe niemals pauschal gewährleistet werden**. Daten der öffentlichen Hand seien offenzulegen (**„openness by design"**). Hier sei zwischen verschiedenen Graden der Offenheit zu unterscheiden. Der Grad der möglichen Offenheit ergebe sich im Wesentlichen aus dem Risiko für die Rechte und Interessen der von der Datenverarbeitung Betroffenen. Es seien zudem die fünf Risikodimensionen eines Datenzugangs des sog. **„Five Safes Model"** (Safe projects, Safe people. Safe data, Safe Settings, Safe outputs) zu berücksichtigen und idealerweise regukatorisch zu beantworten. Weiterhin solle sich der Datenzugang an den **FAIR-Prinzipien** (findable, accessible, interoperable, reusable) orientieren.

De lege lata könne ein Datenzugang für die Wissenschaft über fünf strukturell verschiedene Regulierungsinstrumente erreicht werden: Einen grundrechtsunmittelbaren Datenzugangsanspruch zugunsten der Forschung, echte Forschungsklauseln, Open-Data-Gesetzgebung-Transparenzregelungen und Berichtspflichten sowie Erlaubnisse der Datenzugangsgewährung. Diese Wege würden sich in der Intensivität ihrer Wirkung für die Wissenschaft unterscheiden. Wegen ihrer Werkintensität seien dabei Forschungsklauseln, wie sie bisher in den Sektoren Online-Wirtschaft, Gesundheit und Mobilität bestehen, hervorzuheben. Bezüglich der erfassten Daten und der Zugangsadressatzen sei der Anwendugsbereich dieser Klauseln aber sehr eng. Eine Reihe dieser Forschungsklauseln würde sich zudem durch eine Zweckbindung des Datenzugangs an die wissenschaftliche Forschung auszeichnen.

Aus den grundrechtlichen Rahmenbedingungen, den Prinzipien des Forschungsdatenzugangs und der Analyse der nationalen und internationalen Forschungsklauseln ließen sich sektorspezifische Leitlinien für einen Forschungsdaten-Zugang entwickeln. So sei etwa für ein Gesundheitsforschungsdatengesetz die Normierung einer engen Zweckbindung an gemeinwohlorientierte Forschung zu empfehlen. Im Rechtsvergleich ließe sich auch die Sinnhaftigkeit der Einbindung einer Instanz, die über die ethische Vereinbarkeit der Forschung entscheidet, feststellen.

Der Aufsatz ist (im Rahmen eines beck-online Abos) abrufbar unter:

https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzgi%2F2022%2Fcont%2Fzgi.2022.3.1.htm&pos=1&hlwords=on