

Working Paper

**Datenspende von  
Gesundheitsdaten –  
Nutzen, Risiken und Perspektiven**

Hans-Hermann Dirksen  
Miriam Hamel  
Sophia Scherer  
Cord Spreckelsen  
Felix Wilke  
Michael Zieger

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung



Finanziert von der  
Europäischen Union  
NextGenerationEU

## **Working Paper „Datenspende von Gesundheitsdaten – Nutzen, Risiken und Perspektiven“, Stand 15.04.2024**

**Prof. Dr. Hans-Hermann Dirksen:** Rechtsanwalt, Liebenstein Law – Kanzlei für Wirtschaftsrecht, Frankfurt am Main und FOM Hochschule für Oekonomie und Management, Essen, Professur für das Recht der Digitalisierung.

**Miriam Hamel** (Dipl.-Ing.): Datenschutzbeauftragte Terzo-Institut/ ISMA AG in Sonneberg.

**Sophia Scherer** (cand. jur.): Wissenschaftliche Mitarbeiterin, Liebenstein Law – Kanzlei für Wirtschaftsrecht, Frankfurt am Main.

**Prof. Dr. Cord Spreckelsen:** Universitätsklinikum Jena, Institut für Medizinische Statistik, Informatik und Datenwissenschaften, Professur für Medizinische Informatik.

**Prof. Dr. Felix Wilke:** Ernst-Abbe-Hochschule Jena, Fachbereich Sozialwesen, Professur für Soziologie in der Sozialen Arbeit.

**Dr. Michael Zieger:** SRH Wald-Klinikum Gera GmbH, Zentrum für klinische Studien.

**Das diesem Working Paper zugrundeliegende Vorhaben „AVATAR – Anonymisierung persönlicher Gesundheitsdaten durch Erzeugung digitaler Avatare in Medizin und Pflege“ wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen KIS60FAC004 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autorinnen und Autoren.**

### **Kontakt zum AVATAR – Verbundprojekt**



info@avatar-projekt.de

This article is an open access article distributed under Creative-Commons-Zero (<https://creativecommons.org/publicdomain/zero/1.0/>). You can copy, modify and distribute this work.



## **Inhaltsverzeichnis**

Begriffsdefinition und Hintergrund.....	1
Bedarf für Datenspenden.....	2
Relevanz und Nutzen.....	4
Rechtliche Rahmenbedingungen.....	5
Herausforderungen und Risiken.....	8
Fazit und Perspektiven .....	10
Acknowledgement.....	11

## Begriffsdefinition und Hintergrund

Der Begriff "Datenspende", spezifisch bezogen auf den Bereich der Gesundheitsdaten, beschreibt die freiwillige Bereitstellung oder das Teilen von personenbezogenen Gesundheitsdaten durch individuelle Personen für Forschungszwecke, medizinische Studien oder für die Verbesserung der Gesundheitsversorgung.<sup>1</sup> Die Datenquellen sind vielfältig und umfassen u.a. die medizinische Dokumentation in Krankenhäusern und Praxen (z.B. medizinische Befunde, Bild- und Signaldatensätze, Labordaten), zukünftig auch Daten aus der elektronischen Patientenakte sowie Daten aus tragbaren Gesundheitstechnologien, wie Fitness-Apps oder Smart Watches und damit Informationen aus dem gesamten Bereich Gesundheit, Therapien und Lebensstil.<sup>2</sup> Diese Daten werden freiwillig und zumeist unentgeltlich insbesondere für Forschungszwecke zur Verfügung gestellt, ohne direkten persönlichen Nutzen oder Vorteil für die spendende Person.<sup>3</sup> Die Überlassung der Daten basiert insofern typischerweise auf einer altruistischen Motivation, obwohl in bestimmten Fällen eine Aufwandsentschädigung möglich ist.<sup>4</sup>

Bei Gesundheitsdaten muss die strenge Regulierung durch die EU-Datenschutzgrundverordnung (DSGVO) beachtet werden, die Gesundheitsdaten (Art. 9 DSGVO) als besonders sensible und daher in besonderer Weise schützenswerte Daten definiert. Solche Daten und damit auch die Datenspende unterliegen somit engen Voraussetzungen zur Erhebung und Verarbeitung.

Aufgrund der umfangreichen ethischen Implikationen hat der Deutsche Ethikrat ein Konzept zum Umgang mit Datenspenden im Gesundheitswesen vorgelegt.<sup>5</sup> Dieses Konzept soll an die Systematik und den altruistischen Charakter der Organspende erinnern, indem es die freiwillige und selbstlose Überlassung persönlicher Informationen für das Gemeinwohl hervorhebt.<sup>6</sup> Der Gemeinwohlbezug wird im deutschen Sprachraum durch den Begriff der Spende hervorgehoben. Im angelsächsischen Sprachraum liegt demgegenüber der Fokus eher auf dem Aspekt des Teilens, weshalb dort auch meist von „data sharing“ gesprochen wird.<sup>7</sup>

---

<sup>1</sup> Strech, D., Graf von Kielmansegg, S., Zenker, S., Krawczak, M. & Semler, S. C. (2020) *Wissenschaftliches Gutachten „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen*. Erstellt für das Bundesministerium für Gesundheit. Verfügbar unter <https://www.bundesgesundheitsministerium.de/service/publikationen/details/datenspende-bedarf-fuer-die-forschung-ethische-bewertung-rechtliche-informationstechnologische-und-organisatorische-rahmenbedingungen>

<sup>2</sup> Canali, S., Schiaffonati, V. & Aliverti, A. (2022). Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. *PLOS Digital Health*, 1(10): e000104. <https://doi.org/10.1371/journal.pdig.000104>

<sup>3</sup> Hummel, P., Braun, M., Augsburg, S., Ulmenstein, U.v. & Dabrock, P. (2021). Datensouveränität als informationelle Freiheitsgestaltung. In: *Datensouveränität – Governance-Ansätze für den Gesundheitsbereich* (S. 1-12). Wiesbaden: essentials. Springer VS. [https://doi.org/10.1007/978-3-658-33755-1\\_1](https://doi.org/10.1007/978-3-658-33755-1_1)

<sup>4</sup> Hagen, P. & Völzmann, L. (2022). Datenaltruismus aus datenschutzrechtlicher Perspektive. *MMR - Zeitschrift für IT-Recht und Recht der Digitalisierung*, 3, 176.

<sup>5</sup> Deutscher Ethikrat (2023). *Ethikrat: Gesundheitsdaten besser nutzen, ohne Datenschutz zu schwächen*. 21.03.2023, verfügbar unter: <https://www.ethikrat.org/mitteilungen/mitteilungen/2023/ethikrat-gesundheitsdaten-besser-nutzen-ohne-datenschutz-zu-schwaechen/>

<sup>6</sup> Veil, W. (2020). *Beim Datenaltruismus verpasst die EU eine Chance*. 03.12.2020, verfügbar unter: <https://background.tagesspiegel.de/digitalisierung/beim-datenaltruismus-verpasst-die-eu-eine-chance>

<sup>7</sup> van Panhuis, W. G., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., Herbst, A. J., Heymann, D. & Burke, D. S. (2014). A systematic review of barriers to data sharing in public health, *BMC Public Health*, 14(1), 1144. <https://doi.org/10.1186/1471-2458-14-1144>

## Bedarf für Datenspenden

Gesundheitsdaten sind von zentraler Bedeutung für die biomedizinische Forschung und das öffentliche Gesundheitswesen, mit dem Ziel, die Prävention, Diagnostik und Therapie von Patienten zu verbessern.<sup>8</sup> Sie dienen als wesentliche Informationsquelle, um das Verständnis von Krankheitsbildern zu vertiefen und die Gesundheitsversorgung effizienter zu gestalten. Dies umfasst die aktuelle und zukünftige medizinische Versorgung der Bevölkerung, die Entscheidungsfindung sowie die Aufrechterhaltung der öffentlichen Gesundheit.<sup>9</sup>

Der Bedarf an Datenspenden begründet sich in dem Wunsch, wissenschaftliche Erkenntnisse schneller zu erweitern und medizinischen Fortschritt zu fördern. Dies gelingt durch die Bereitstellung großer Mengen an Gesundheitsdaten, da zum einen auf bereits vorhandene Daten zurückgegriffen werden kann<sup>10</sup> und zum anderen zuverlässigere Auswertungen erfolgen können. Dies reduziert nicht nur den Zeitaufwand für die Datenerhebung, sondern vermindert auch potenzielle Belastungen für Patienten durch zusätzliche Untersuchungen in klinischen Studien.<sup>11</sup>

Mit der Digitalisierung ergeben sich umfassende Möglichkeiten, Gesundheitsdaten für den medizinischen Fortschritt sowie die Entwicklung neuer Behandlungsansätze nutzbar zu machen.<sup>12</sup> Bei der Nutzung von Datenspenden ist jedoch auf die Qualität und Vergleichbarkeit der Daten zu achten.<sup>13</sup> Dies schließt die Sicherstellung der Repräsentativität (die Daten bilden die Bevölkerungsgruppe, aus der sie erhoben wurden, ausgewogen ab) und Validität (die Daten sind inhaltlich zutreffend) der Daten ein. Durch die Einhaltung dieser Standards wird gewährleistet, dass die Forschungsergebnisse zuverlässig und aussagekräftig sind.

## Bereitschaft zu Datenspenden

Die gesellschaftliche Aufmerksamkeit für das Thema der Datenspende hat in den letzten Jahren erheblich zugenommen. Dies spiegelt sich beispielsweise in der großen Teilnahme an Projekten, wie der Corona-Datenspende-App des Robert-Koch-Instituts, wider, bei der über 500.000 Menschen ihre Gesundheitsdaten zur Verfügung gestellt haben.<sup>14,15</sup>

---

<sup>8</sup> Bundesministerium für Gesundheit (2024). *Daten für die Forschung und Versorgung*. 19.01.2024, verfügbar unter: <https://www.bundesgesundheitsministerium.de/themen/digitalisierung/daten-fuer-die-forschung-und-versorgung>

<sup>9</sup> Chen, H., Hailey, D., Wang, N. & Yu, P. (2014). A Review of Data Quality Assessment Methods for Public Health Information Systems. *International Journal of Environmental Research and Public Health*, 11(5), 5170-5207. <https://doi.org/10.3390/ijerph110505170>

<sup>10</sup> Huston, P., Edge, V. L., & Bernier, E. (2019). Reaping the benefits of open data in public health. *Canada Communicable Disease Report*, 45(11), 252-256. <https://doi.org/10.14745/ccdr.v45i10a01>

<sup>11</sup> Springer, S., Zieger, M. & Strzelecki, A. (2021). The rise of infodemiology and infoveillance during COVID-19 crisis. *One Health*, 13, 100288. <https://doi.org/10.1016/j.onehlt.2021.100288>

<sup>12</sup> Thiel, R. & Deimel, L. (2022). *Forschungsdatenfreigabe von ePA-Daten in Europa*. Gütersloh: Bertelsmann Stiftung.

<sup>13</sup> Health Metrics Network & World Health Organization (2008). *Framework and standards for country health information systems*, 2nd ed. Geneva, Switzerland: World Health Organization.

<sup>14</sup> Kölling, A. & Mossig, M. (2021). *Hohe Bereitschaft zur Spende von Gesundheitsdaten*. 16.07.2021, verfügbar unter: <https://www.uni-bremen.de/hohe-bereitschaft-zur-spende-von-gesundheitsdaten>

<sup>15</sup> Robert Koch Institut (2021). *Corona-Datenspende 2.0 - Robert Koch-Institut startet App-Studien zu Pandemie-Langzeitfolgen*. 19.10.2021, verfügbar unter: [https://www.rki.de/DE/Content/InfAZ/N/Neuartiges\\_Coronavirus/Corona-Datenspende-2-0.html](https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende-2-0.html)

Doch die Bereitschaft zur Spende persönlicher Gesundheitsdaten unterscheidet sich erheblich zwischen verschiedenen Ländern und Personengruppen.<sup>16</sup> Ein wesentlicher Faktor sind institutionelle und kulturelle Unterschiede. Im europäischen Kontext zeichnen sich insbesondere die nordeuropäischen Länder durch eine hohe Bereitschaft zur Spende von Gesundheitsdaten aus.<sup>12</sup> In diesen Ländern ist die Digitalisierung des Gesundheitswesens weiter vorangeschritten als in vielen anderen europäischen Ländern. Auch existiert dort bereits eine in der Breite zugängliche Infrastruktur, um Gesundheitsdaten zu spenden.<sup>12</sup>

Hinsichtlich der Bereitschaft zur Spende von Gesundheitsdaten in Deutschland zeigen Bevölkerungsbefragungen bislang keine eindeutigen Befunde. In Umfragedaten schwanken die Zustimmungsraten bei Datenspenden für Forschungszwecke zwischen 20% und 80%.<sup>16,17,18</sup> In dieses Bild reihen sich neue Befragungsdaten zur elektronischen Patientenakte ein. Diese zeigen, dass ca. 50% der Bevölkerung einer Datenspende positiv gegenüberstehen.<sup>19</sup> Die Spendenbereitschaft unterliegt innerhalb der Bevölkerung zum Teil erheblichen sozialen Ungleichheiten. Aus der internationalen Forschung ist bekannt, dass Personen im jüngerem Lebensalter<sup>17,20,21</sup>, mit höherer Bildung<sup>17,22,23</sup> und höherem Einkommen<sup>22</sup> häufiger zur Datenspende bereit sind. Zudem sind Personen eher bereit, ihre Daten zu teilen, wenn sie dem Datentreuhänder vertrauen und glauben, dass ihre Daten sicher und verantwortungsvoll behandelt werden.<sup>17,23</sup> Trotz einer generellen Bereitschaft zur Datenspende stellen Bedenken hinsichtlich des Datenschutzes und der Privatsphäre wichtige Hürden dar.

Datenspenden setzen regelmäßig die Nutzung digitaler Anwendungen auf Seiten der Bürger voraus (z.B. Corona-Datenspende-App, Apple Health, Google Health usw.). Es überrascht deshalb wenig, dass die Bereitschaft zur Datenspende auch mit der digitalen Affinität der Bürger in einem engen Zusammenhang steht. Personen mit einer hohen digitalen Kompetenz bzw. Erfahrungen

---

<sup>16</sup> Karampela, M., Ouhbi, S. & Isomursu, M. (2019). Connected Health User Willingness to Share Personal Health Data: Questionnaire Study. *Journal of Medical Internet Research*, 21 (11), e14537. <https://doi.org/10.2196/14537>

<sup>17</sup> Semler, Sebastian C. (2019). „Datenspende“ für die medizinische Forschung: Ergebnisse einer aktuellen Umfrage. TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (MII-Workshop „Gesundheitsdaten für die medizinische Forschung: Wie können Patienten partizipieren?“). 27.08.2019, verfügbar unter [https://www.tmf-ev.de/sites/default/files/2023-05/sebastian\\_semler\\_ergebnisse\\_einer\\_aktuellen\\_umfrage.pdf](https://www.tmf-ev.de/sites/default/files/2023-05/sebastian_semler_ergebnisse_einer_aktuellen_umfrage.pdf)

<sup>18</sup> Kühnel, E. & Wilke, F. (im Druck). Potentiale der Digitalisierung heben: Die Bereitschaft zur Spende von Gesundheitsdaten in Deutschland und Finnland. In: K. T. Heckes, M. Lorke, M. Siegler und K. J. Wrona (Hrsg.), *Soziotechnische Transformationen im Sozial und Gesundheitswesen: kollaborativ, divers, barrierefrei und sozialräumlich*. Beltz Juventa.

<sup>19</sup> Kühnel, E., Wilke, F. & Berghäuser, J (2024). *Meine Gesundheitsdaten für die Forschung? - Neue Befunde aus einer repräsentativen Befragung zur Datenspende mittels elektronischer Patientenakte*. 25.03.2024, verfügbar unter: [https://www.eah-jena.de/fileadmin/user\\_upload/projecte/avatar/Meine\\_Gesundheitsdaten\\_fuer\\_die\\_Forschung.pdf](https://www.eah-jena.de/fileadmin/user_upload/projecte/avatar/Meine_Gesundheitsdaten_fuer_die_Forschung.pdf)

<sup>20</sup> Weng, C., Friedman, C., Rommel, C. A., Hurdle, J. F. (2019). A two-site survey of medical center personnel's willingness to share clinical data for research: implications for reproducible health NLP research. *BMC medical informatics and decision making*, 19 (Suppl 3), 70. <https://doi.org/10.1186/s12911-019-0778-z>

<sup>21</sup> Broekstra, R., Aris-Meijer, J. L., Maeckelberghe, E. L. M., Stolk, R.P. & Otten, S. (2022). Motives for withdrawal of participation in biobanking and participants' willingness to allow linkages of their data. *European Journal of Human Genetics*, 30 (3), 367-377. <https://doi.org/10.1038/s41431-021-00997-5>

<sup>22</sup> Moon, L. A. (2017). Factors influencing health data sharing preferences of consumers: A critical review. *Health Policy and Technology*, 6 (2), 169-187. <https://doi.org/10.1016/j.hlpt.2017.01.001>

<sup>23</sup> Bosanac, D. & Stevanovic, A. (2022). Trust in E-Health System and Willingness to Share Personal Health Data. *Studies in Health Technology and Informatics*, 289, 256-259. <https://doi.org/10.3233/SHTI210908>

mit digitalen Technologien und Anwendungen - insbesondere im Gesundheitsbereich - sind eher bereit, Gesundheitsdaten über digitale Verfahren zu teilen.<sup>23,24</sup>

Aus der unterschiedlichen Spendenbereitschaft in der Bevölkerung, die sich u.a. aus dem „digital divide“ ergibt<sup>25</sup>, erwachsen Probleme und Herausforderungen für die Datenqualität, die zu einem eingeschränkten Nutzen von Datenspenden führen können. Die Selektivität gespendeter Gesundheitsdaten vermindert die Datenqualität und schränkt das Spektrum der Nutzungsmöglichkeiten ein.

## Relevanz und Nutzen

Die Datenspende im Gesundheitsbereich hat eine erhebliche Bedeutung für fast alle Aspekte der medizinischen Forschung und Gesundheitsversorgung.<sup>26</sup> Im Bereich der medizinischen Forschung zeigt sich, dass es der Zugang zu umfangreichen Gesundheitsdatensätzen ermöglicht, Muster und Trends bei Krankheiten effektiver zu erkennen.<sup>24</sup> Dies fördert die Entwicklung innovativer Behandlungsmethoden und trägt zur Optimierung der Patientenversorgung bei.<sup>27</sup> Die Verfügbarkeit dieser Daten kann den Forschungsprozess erheblich beschleunigen und zu wichtigen Durchbrüchen in der Medizin führen.<sup>28</sup>

Große Datenmengen aus Datenspenden erlauben im Anwendungsfeld der personalisierten Medizin eine präzisere, statistisch abgesicherte Analyse, die auch zur Entwicklung von maßgeschneiderten, auf den einzelnen Patienten zugeschnittenen, Behandlungsstrategien führt.<sup>29,30</sup> Dies bedeutet eine erhebliche Verbesserung in der Effektivität der medizinischen Behandlung, da sie spezifische genetische, umweltbedingte und persönliche Faktoren berücksichtigen kann.<sup>31</sup>

Der Zugang zu Gesundheitsdatensätzen aus Datenspenden kann einen wesentlichen Beitrag zur Überwachung und Bekämpfung von Volkskrankheiten leisten. So können Gesundheitsdienste besser geplant und koordiniert werden, indem Trends und Risikofaktoren aufgezeigt werden können<sup>32</sup>, was zu effektiveren Präventions- und Interventionsstrategien im Bereich der öffentlichen Gesundheit führt<sup>24</sup>.

---

<sup>24</sup> Saegner, T. & Austys, D. (2022). Forecasting and surveillance of COVID-19 spread using Google trends: literature review. *International Journal of Environmental Research and Public Health*, 19(19), 12394. <https://doi.org/10.3390/ijerph191912394>

<sup>25</sup> Lupton, D. (2018). *Digital health*. London: Routledge, Taylor & Francis Group.

<sup>26</sup> Strotbaum, V., Pobiruchin, M., Schreiweis, B., Wiesner, M., & Strahwald, B. (2019). Your data is gold – Data donation for better healthcare?. *It-Information Technology*, 61(5-6), 219-229. <https://doi.org/10.1515/itit-2019-0024>

<sup>27</sup> Mooney, S. J. & Pejaver, V. (2018). Big data in public health: terminology, machine learning, and privacy. *Annual review of public health*, 39, 95-112. <https://doi.org/10.1146/annurev-publhealth-040617-014208>

<sup>28</sup> Issa, N. T., Byers, S. W., & Dakshanamurthy, S. (2014). Big data: the next frontier for innovation in therapeutics and healthcare. *Expert Review of Clinical Pharmacology*, 7(3), 293-298. <https://doi.org/10.1586/17512433.2014.905201>

<sup>29</sup> Chawla, N. V. & Davis, D. A. (2013). Bringing big data to personalized healthcare: a patient-centered framework. *Journal of General Internal Medicine*, 28, 660-665. <https://doi.org/10.1007/s11606-013-2455-8>

<sup>30</sup> Viceconti, M., Hunter, P. & Hose, R. (2015). Big Data, Big Knowledge: Big Data for Personalized Healthcare. *IEEE Journal of Biomedical and Health Informatics*, 19(4), 1209-1215. <https://doi.org/10.1109/JBHI.2015.2406883>

<sup>31</sup> Rauter, C. M., Wöhlke, S. & Schickanz, S. (2021). My Data, My Choice? – German Patient Organizations' Attitudes towards Big Data-Driven Approaches in Personalized Medicine. An Empirical-Ethical Study. *Journal of Medical Systems*, 45, 43. <https://doi.org/10.1007/s10916-020-01702-7>

<sup>32</sup> Springer, S., Strzelecki, A. & Zieger, M. (2023). Maximum generable interest: A universal standard for Google Trends search queries. *Healthcare Analytics*, 3, 100158. <https://doi.org/10.1016/j.health.2023.100158>

## Rechtliche Rahmenbedingungen

Die Datenspende wirft komplexe juristische Fragen auf, insbesondere im Hinblick auf den Datenschutz, die Datensicherheit und die Repräsentativität der Daten.

Bevor in Deutschland bestehende medizinische Datensätze für die Forschung weiterverwendet werden können, ist es erforderlich, die rechtlichen und infrastrukturellen Rahmenbedingungen zu bestimmen. Einerseits sichert das Grundgesetz (GG) das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG), andererseits gewährleistet es die Freiheit der Wissenschaft (Art. 5 Abs. 3 GG). Konkret wird die Nutzung von personenbezogenen medizinischen Daten gegenwärtig durch einen einheitlichen europäischen Rechtsrahmen reguliert, der die Verarbeitung dieser Daten steuert.

Bedeutsam ist zunächst, dass Gesundheitsdaten nicht als persönliches Eigentum im Sinne des Sachenrechts des Bürgerlichen Gesetzbuches (BGB) angesehen werden. Personen erhalten zwar bestimmte Rechte an ihren Daten, wie das Recht auf Zugang, Berichtigung, Löschung und das Recht, die Verarbeitung einzuschränken, aber kein „Dateneigentum“ im herkömmlichen Sinne.<sup>33</sup> Die Rechte an ihren Daten ermöglichen es den Personen, Kontrolle über ihre Gesundheitsdaten auszuüben.<sup>34</sup> Es bedeutet aber auch, dass Daten nicht einfach wie bewegliche Sachen im eigentumsrechtlichen Sinne verschenkt bzw. gespendet werden können.<sup>35</sup> Der Begriff der "Datenspende" ist daher aus rechtlicher Perspektive eher eine metaphorische Umschreibung dafür, dass eine Person der Verarbeitung und Nutzung ihrer persönlichen Daten für bestimmte Zwecke (z.B. Forschung) zustimmt.

Einige ausländische Rechtssysteme haben dagegen begonnen, Daten als "digitale Objekte"<sup>36</sup> oder "Digitalinhalte" zu betrachten und eigene rechtliche Regelungen für sie zu schaffen.<sup>37</sup>

Gemäß der europäischen Datenschutz-Grundverordnung (DSGVO) und auch dem Bundesdatenschutzgesetz (BDSG) sind persönliche Daten und insbesondere Gesundheitsdaten als besondere Kategorien personenbezogener Daten geschützt und ihre Verarbeitung ist an klare Voraussetzungen gebunden, die in Deutschland durch § 22 BDSG in umfangreicher Weise ergänzend geregelt wird. Dies beinhaltet die Notwendigkeit der Transparenz in der Datenerhebung, -verarbeitung und -nutzung sowie die Implementierung angemessener Sicherheitsmaßnahmen zum Schutz der Daten.<sup>38</sup>

---

<sup>33</sup> Hoeren, T. (2023): Alibaba und das Dateneigentum – 25 Jahre später. *MMR - Zeitschrift für IT-Recht und Recht der Digitalisierung*, 1, 32.

<sup>34</sup> Bundesministerium für Wirtschaft und Klimaschutz (ohne Jahr). *FAQ Datenhoheit*. Verfügbar unter: <https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/FAQ-Recht/datenhoheit.html>

<sup>35</sup> Matern, S. (2023). *Datenschutz im Gesundheitswesen: Ein Blick auf Gesundheitsdaten und die DSGVO*. 15.11.2023, verfügbar unter: <https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/datenschutz-im-gesundheitswesen/>

<sup>36</sup> Müller, K. (2018). Digitale Objekte – subjektive Materie. Zur Materialität digitalisierter Objekte in Museum und Archiv. In H. Hahn & F. Neumann (Hrsg.), *Dinge als Herausforderung: Kontexte, Umgangsweisen und Umwertungen von Objekten* (S. 49-66). Bielefeld: transcript Verlag. <https://doi.org/10.1515/9783839445136-004>

<sup>37</sup> Bucaria, G. (2021). *Digital Objects as Suitable Objects of Property Law: Tensions within the System* (Master Thesis). Verfügbar unter: <https://etd.adm.unipi.it/etd-05072021-195228/>

<sup>38</sup> Thüsing, G. & Rombey, S. (2019). Forschung im Gesundheitswesen: Anforderungen an einen passgenauen Datenschutz, *NZS - Neue Zeitschrift für Sozialrecht*, 6, 201.



Gesundheitsdaten sind dabei nach Definition des Art. 9 DSGVO und gemäß Erwägungsgrund 35 DSGVO personenbezogene Daten, „die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen und geistigen Gesundheitszustand der betroffenen Person hervorgehen“. Es handelt sich dabei um hochsensible Daten, die deshalb einem besonderen Schutz unterliegen.

Sofern also solche Kategorien von Daten erhoben, gespeichert und verarbeitet werden sollen und keine der in § 22 BDSG genannten Voraussetzungen, wie zum Beispiel ein medizinisches Behandlungsverhältnis vorliegt, ist eine freiwillige und informierte Einwilligung des Datenlieferanten eine grundlegende Voraussetzung. Die Einwilligung muss dabei den Anforderungen der Art. 9 Abs. 2 lit. a i.V.m. Art. 4 Nr. 11 und Art. 7 DSGVO entsprechen und es muss sichergestellt werden, dass die Personen ihre Rechte und die Verwendung ihrer Daten verstehen (Art. 12 Abs. 1 DSGVO).

Die DSGVO fordert in diesem Zusammenhang, dass die Zustimmung auf der Grundlage vollständiger Information erfolgt. Die Einwilligung muss zudem für bestimmte, ausdrücklich genannte Zwecke erfolgen. Das Problem hierbei ist, dass breit gefasste oder vage Zustimmungen nicht den Anforderungen der DSGVO entsprechen. Datenspender müssen genau verstehen, welche Daten wie verwendet werden.

Häufig sind aber die wissenschaftlichen Fragestellungen, für die sich die erhobenen Daten eignen könnten, zum Zeitpunkt der Datenerhebung noch gar nicht vollständig definiert. Weiterhin können im Verlauf der Forschungsaktivitäten neue Fragestellungen auftauchen, die zu Beginn ebenso unvorhersehbar waren wie die Identifizierung der am besten dafür qualifizierten und geeigneten Einrichtungen. Die COVID-19-Pandemie hat diese Herausforderungen besonders klar hervorgehoben.

Ein Lösungsansatz für dieses Problem stellt der sog. „broad consent“ („breite“ Einwilligung) dar, also eine Zustimmung, die nicht auf ein spezifisches Forschungsprojekt begrenzt ist. Eine solche Form der Einwilligung wird in Erwägungsgrund 33 der DSGVO explizit erwähnt und wurde durch die vom BMBF geförderte Medizininformatik-Initiative (MI-I) in Zusammenarbeit mit der Bundesdatenschutzkonferenz entwickelt, um routinemäßig erhobene Gesundheitsdaten datenschutzgerecht für die Forschung nutzbar zu machen.<sup>39</sup>

Diese „breite“ Einwilligung ist dabei nicht an einen einzigen bestimmten Forschungszweck gebunden, solange die Datennutzungsvorhaben der medizinischen Forschung, wie in den Einwilligungsdokumenten beschrieben, dienen. Dies wird für jedes einzelne Projekt durch eine Ethikkommission sowie sog. „Data Use & Access Committees“ überprüft.<sup>40</sup>

Die DSGVO verlangt zudem, dass die Einwilligung nachweisbar ist. Einrichtungen müssen also in der Lage sein, die Zustimmung einer Person zu dokumentieren und bei Bedarf nachweisen zu können. Dies kann insbesondere bei großen Datenmengen oder bei Datenspenden über digitale Plattformen eine Herausforderung darstellen.

---

<sup>39</sup> Weiterführende Informationen zur Medizininformatik-Initiative sind verfügbar unter: <https://www.medizininformatik-initiative.de/de/start>

<sup>40</sup> Weiterführende Informationen und das Musterdokument für die „breite“ Einwilligung sind verfügbar unter: <https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung>

Gemäß den rechtlichen Grundlagen kann eine Datenspende allerdings auch wieder zurückgenommen werden, welches naturgemäß ein Risiko für die Forschung darstellt.<sup>41</sup> Dies ist auf das Recht auf Widerruf der Einwilligung zurückzuführen, das in Art. 7 Abs. 3 DSGVO verankert ist. Ein Widerruf hat zur Folge, dass die weitere Verarbeitung der Daten für die spezifischen Zwecke, für die sie gespendet wurden, ab dem Zeitpunkt des Widerrufs nicht mehr zulässig ist. Es ist zu beachten, dass der Widerruf der Einwilligung aber nicht rückwirkend und ebenfalls nicht für anonymisierte Daten gilt. Das bedeutet, dass eine Verarbeitung in der Forschung, die bis zum Widerruf erfolgt ist, sowie die Verarbeitung anonymer Daten rechtlich zulässig bleibt.<sup>42</sup>

Im März 2024 ist das Gesetz zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz - GDNG) in Kraft getreten, welches mehr Struktur im Umgang mit Gesundheitsdaten schaffen soll.<sup>43,44</sup> So soll eine zentrale Datenzugangs- und Koordinationsstelle eingerichtet werden, die den Zugang zu Forschungsdaten aus verschiedenen Datenquellen über Forschungspseudonyme ermöglichen soll. Dabei sollen pseudonymisierte Gesundheitsdaten aus der elektronischen Patientenakte automatisch über ein Forschungsdatenzentrum zu Forschungszwecken in geschützten Umgebungen abrufbar gemacht werden.<sup>42</sup>

Allerdings sieht die Erlaubnisregelung in § 6 Abs. 3 GDNG nur eine gemeinsame standortübergreifende Nutzung vor. Eine Herausgabe an eine eigenverantwortlich tätige externe Einrichtung könnte davon ggf. schon nicht mehr abgedeckt sein.

Zudem wurde der seit dem 24. September 2023 in den EU-Mitgliedstaaten unmittelbar geltende Data Governance Act (DGA) erlassen, welcher in Kapitel IV (Art. 16 ff. DGA) den Begriff des Datenaltruismus regelt. Ziele dieses Rechtsaktes der Europäischen Kommission sind unter anderem die Einführung eines nationalen öffentlichen Registers von anerkannten datenaltruistischen Organisationen (Art. 17 ff. DGA) und der Erlass eines europäischen Einwilligungsformulars zum Datenaltruismus (Art. 25 DGA). Allerdings bedürfen die Zugangsrechte zu Daten bestimmten Datensätzen oder Dokumenten einer nationalen Konkretisierung.<sup>45</sup>

Für die Datenspende im Rahmen der EU-Gesetzgebung, insbesondere im Kontext der DSGVO und des DGA, erfolgt keine wesentliche Vereinfachung der rechtlichen Rahmenbedingungen. Trotz der Zielsetzung, Daten zu altruistischen Zwecken zu verarbeiten, bleiben die strengen Vorgaben der DSGVO bestehen. Der DGA bietet keine spezifischen Regelungen zum Prozess der Datenspende.<sup>4</sup> Stattdessen führt er zusätzliche formelle Anforderungen und eine neue behördliche Überprüfungsinstanz ein. Diese Überlappung der Regelungsbereiche von DSGVO und DGA könnte den bürokratischen Aufwand für Organisationen, die sich auf datenaltruistische Aktivitäten konzentrieren, eher noch erhöhen. Trotz möglicher Vorteile, wie der Standardisierung durch

---

<sup>41</sup> Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit - BfDI (2020). *Statement des BfDI zur Corona-Datenspende-App*. 07.04.2020, verfügbar unter: [https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2020/09\\_Statement-Datenspende-App-RKI.html](https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2020/09_Statement-Datenspende-App-RKI.html)

<sup>42</sup> Lorenz, L. (2023). Die „ePA für alle“ zwischen Gesundheits- und Datenschutz (Teil 1). *GuP - Gesundheit u. Pflege*, 4, 132.

<sup>43</sup> Bundesministerium für Gesundheit. (2023). *Gesundheitsdatennutzungsgesetz (GDNG)*. 14.12.2023, verfügbar unter: <https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/gesundheitsdatennutzungsgesetz.html>

<sup>44</sup> Gesetzesbeschluss des Deutschen Bundestages. (2024). *Gesetz zur verbesserten Nutzung von Gesundheitsdaten*. 12.01.2024, verfügbar unter: <https://dserver.bundestag.de/brd/2024/0003-24.pdf>

<sup>45</sup> European Commission (2024). *Data Governance Act explained*. 25.01.2024, verfügbar unter: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained>

Musterformulare und dem Aufbau von Vertrauen durch ein entsprechendes Logo, scheint der Mehrwert dieser Maßnahmen begrenzt.<sup>46</sup>

## Herausforderungen und Risiken

Da es sich bei Gesundheitsdaten um besonders sensible und schützenswerte Daten handelt, birgt deren Spende auch bestimmte Risiken. Es lassen sich unmittelbare Risiken des Datenschutzes und die Gefahr von Re-Identifizierung auf der einen Seite und mittelbare Risiken der unerwünschten Verwendung der Gesundheitsdaten auf der anderen Seite unterscheiden.

### ***Unmittelbare Risiken des Datenschutzes und die Gefahr von Re-Identifizierung***

Für Organisationen und Forschungseinrichtungen, die Daten für wissenschaftliche oder gemeinnützige Zwecke sammeln, gelten spezielle Regelungen, um sicherzustellen, dass die Datenspende in Übereinstimmung mit den Datenschutzbestimmungen erfolgt.<sup>47,48</sup> Dazu gehört beispielsweise die Anonymisierung oder Pseudonymisierung der gespendeten Daten, um die Privatsphäre und den Datenschutz der spendenden Person zu gewährleisten.<sup>49</sup>

Bei der Anonymisierung werden alle Merkmale, die eine natürliche Person direkt oder indirekt identifizieren, gelöscht oder so verändert, dass sie nicht mehr auf die Person zutreffen. Sind Daten korrekt anonymisiert, kann niemand mehr Rückschlüsse auf die Person ziehen, von der die Daten stammen, auch nicht die Institution, die die Daten erhoben hat. Anonymisierte Daten unterliegen dann nicht mehr dem Schutz der DSGVO, wodurch sich beispielsweise ein Widerruf einer Einwilligung nicht auf solche Daten auswirken kann.

Für die Pseudonymisierung werden im Gegensatz zur Anonymisierung eindeutig identifizierende Merkmale durch Pseudonyme (z.B. Codes als Kombinationen aus Buchstaben und Zahlen) ersetzt. Die Zuordnung der Pseudonyme zu den originalen Merkmalen wird in einer gesonderten Ablage gespeichert. Durch pseudonymisierte Daten ist es beispielsweise möglich, Daten aus mehreren Quellen zusammenzuführen. Auch bei der Pseudonymisierung können einzelne Merkmale verändert oder gelöscht werden, um eine indirekte Identifizierung möglichst auszuschließen. Da allerdings pseudonymisierte Daten nach wie vor unter die DSGVO fallen, müssen sie weiterhin mit angemessenen Mitteln geschützt werden. Ebenfalls unterliegen sie den Betroffenenrechten (z.B. Recht auf Auskunft, Recht auf Einschränkung der Verarbeitung, Recht auf Löschung).<sup>50</sup>

Bei beiden Maßnahmen kann jedoch eine Re-Identifizierung, also die Rückführung anonymisierter oder pseudonymisierter Daten auf die ursprüngliche Person, nicht vollständig ausgeschlossen werden.<sup>51</sup> Dieses Risiko kann sich aus verschiedenen technischen Anwendungen ergeben,

---

<sup>46</sup> Heinzke, P. (2023). Data Act: Auf dem Weg zur europäischen Datenwirtschaft, *BB - BetriebsBerater*, 5, 201.

<sup>47</sup> Weichert, T. (2020). Die Forschungsprivilegierung in der DS-GVO. *ZD - Zeitschrift für Datenschutz*, 1, 18.

<sup>48</sup> Rosnagel, A. (2019). Datenschutz in der Forschung. *ZD - Zeitschrift für Datenschutz*, 4, 157.

<sup>49</sup> Jones, C. (2020). Datenschutzrechtliche Herausforderungen für Ärzte beim Einsatz von Gesundheits-Apps. *Deutsche Stiftung für Recht und Informatik Tagungsband (DSRITB)*, 1, 127.

<sup>50</sup> Bischoff, C. & Drechsler, J. (2020). Pseudonymisierung und Anonymisierung im Rahmen klinischer Prüfungen von Arzneimitteln (Teil II). *PharmR - Fachzeitschrift für das gesamte Arzneimittelrecht*, 7, 389.

<sup>51</sup> Stummer, S. (2023). Identifizierbarkeit und Anonymität im Internet. *ZfDR - Zeitschrift für Digitalisierung und Recht*, 3, 263.

darunter die Verknüpfung von Daten, die Verwendung von Metadaten oder auch die Veröffentlichung scheinbar harmloser Informationen, die in Kombination mit anderen Informationen zur Identifizierung einer Person führen können.<sup>52,53,54</sup>

Um das Re-Identifizierungsrisiko zu minimieren, sind insofern technische und organisatorische Sicherheitsmaßnahmen und Richtlinien erforderlich. Organisationen und Unternehmen müssen sicherstellen, dass sie strenge Sicherheitsprotokolle implementieren, um den Zugang zu sensiblen Daten an sich zu beschränken und die Verwendung von speziellen Sicherheitstechnologien fördern, die eine sichere Verarbeitung und Speicherung gewährleisten. Darüber hinaus ist es von Bedeutung, dass die Verantwortlichen entsprechend geschult werden, um die Risiken der Re-Identifizierung möglichst auszuschließen.<sup>55</sup>

Insgesamt erfordert die Handhabung von Datenspenden daher eine sorgfältige Abwägung von Datenschutzerfordernissen aber auch ethischen Erwägungen, um die Privatsphäre durch Schutz der Grundrechte und Grundfreiheiten der natürlichen Personen (Datenspender) zu wahren aber gleichzeitig den wissenschaftlichen Nutzen erfolgreich zu maximieren.<sup>56</sup> Nur so kann gewährleistet werden, dass die dringend notwendige Bereitschaft zu Datenspenden erhalten und bestenfalls sogar gefördert wird.

### **Mittelbare Risiken der Verwendung von Gesundheitsdaten**

Re-Identifizierungsrisiken und die Notwendigkeit eines guten Datenschutzes, verweisen bereits auf das Risiko einer missbräuchlichen Verwendung von Gesundheitsdaten. So können öffentlich bekannt werdende oder veröffentlichte Gesundheitsdaten zum Nachteil der Datenspender eingesetzt werden. Diskriminierung am Arbeitsmarkt, Änderungen beim Versicherungsschutz oder auch Strafverfolgung sind einige Beispiele dafür (z.B. Daten aus Zyklus-Apps als Beleg für einen illegalen Schwangerschaftsabbruch<sup>57</sup>). Veröffentlichte genetische Informationen können zu einer Identifizierung des Datenspenders oder seiner Verwandten führen.<sup>58</sup> Bei posthumen Datenspenden steht zudem das Risiko eines Kontrollverlusts im Raum.<sup>59</sup>

Würden Konzepte der Datenspende in Deutschland vor allem vor dem Hintergrund der öffentlichen Daseinsvorsorge diskutiert, bestehen nun zunehmend Befürchtungen, dass gespendete

---

<sup>52</sup> Office for Civil Rights - OCR. (2012). *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*. 26.11.2012, verfügbar unter: <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>

<sup>53</sup> Schwan, C. (2020). *RKI-App „Corona-Datenspende“ – Wie „freiwillig“ ist die Einwilligung?* 07.04.2020, verfügbar unter: <https://www.dr-datenschutz.de/rki-app-corona-datenspende-wie-freiwillig-ist-die-einwilligung/>

<sup>54</sup> Schirnbacher, M., Lewald, A. & Czempinski, M. (2023). *Wenn schon teilen dann richtig – Der Data Governance Act*. 23.11.2023, verfügbar unter: <https://haerting.de/wissen/wenn-schon-teilen-dann-richtig-der-data-governance-act/>

<sup>55</sup> Bundesverband der Deutschen Industrie e.V. (2020). *Anonymisierung personenbezogener Daten – Ein branchenübergreifender Praxisleitfaden für Industrieunternehmen*. 11.02.2020, verfügbar unter: <https://bdi.eu/publikation/news/anonymisierung-personenbezogener-daten>

<sup>56</sup> Specht-Riemenschneider, L. & Wehde, A. (2022): *Forschungsdatenzugang*. *ZGI - Zeitschrift für das gesamte Informationsrecht*, 1, 3.

<sup>57</sup> Kathe, S. (2023). *US-Abtreibungsgesetze: Wie Zyklus-Apps zum Problem werden*. 27.02.2023, verfügbar unter: <https://www.fr.de/politik/abtreibungsgesetze-in-den-usa-wie-apps-zur-zyklusverfolgung-zum-problem-werden-92112091.html>

<sup>58</sup> Berkman, B. E., Miller, W. K & Grady, C. (2018). *Is It Ethical to Use Genealogy Data to Solve Crimes?* *Annals of Internal Medicine*, 169 (5), 333-334. <https://doi.org/10.7326/M18-1348>

<sup>59</sup> Krutzinna, J., Taddeo, M. & Floridi, L. (2019). *Enabling Posthumous Medical Data Donation: An Appeal for the Ethical Utilisation of Personal Health Data*. *Science and Engineering Ethics*, 25 (5), 1357-1387. <https://doi.org/10.1007/s11948-018-0067-8>

Gesundheitsdaten so in kommerzielle Angebote integriert werden, dass sich Bürger diesen nicht mehr entziehen können. Derzeit expandieren zahlreiche profitorientierte Technologiekonzerne im Bereich der Gesundheitsdaten<sup>25</sup> und erschaffen "soziotechnische Ökosysteme", denen man sich im Alltag immer weniger entziehen kann.<sup>60,61</sup>

Dass Gesundheitsanwendungen vieler Drittanbieter (z.B. von „wearables“, wie Fitnesstrackern) nur über Gesundheitsplattformen einiger weniger Technologiekonzerne in vollem Umfang genutzt werden können, ist ein Zeichen in Richtung geschlossener Ökosysteme.<sup>62</sup> Die Preisgabe von persönlichen Daten seitens der Bürger wird in diesen Ökosystemen eine notwendige Bedingung zur Partizipation. Es besteht die Gefahr, dass Bürger mit ihren Gesundheitsdaten ähnlich pragmatisch wie mit anderen personenbezogenen Daten im Netz umgehen (müssen).<sup>63</sup>

Durch das Sammeln von Daten besteht auch die Gefahr, dass Gesundheitsdaten zur Ausweitung sozialer Kontrolle und Verhaltenssteuerung eingesetzt werden.<sup>25,64</sup> Bürger können sich diesen Entwicklungen nur partiell entziehen. Indem individuelle Vorteile mit der Preisgabe persönlicher Gesundheitsdaten (z.B. Telematik-Tarife) verknüpft werden, weiten sich Möglichkeiten der Fremd- und Selbstkontrolle aus. Das zeigen auch empirische Erfahrungen mit Disease-Management-Programmen, die einerseits integrierte Versorgung verbessern, aber gleichzeitig umfangreiche Datenspenden voraussetzen.<sup>65</sup>

In der Konsequenz zeigt sich also, dass die ethische Dimension von Datenspenden hochkomplex ist und dass der Schutz der persönlichen Daten und die Wahrung der Autonomie der Individuen auch in diesem Zusammenhang zentrale ethische Prinzipien von Forschungseinrichtungen und Gesundheitsdienstleistern sein müssen, um das Vertrauen in die Praxis der Datenspende zu stärken und gleichzeitig den wissenschaftlichen Fortschritt im Einklang mit den ethischen Werten der Gesellschaft zu fördern.

## Fazit und Perspektiven

Die Datenspende im Gesundheitssektor bringt sowohl Chancen als auch Herausforderungen mit sich. Dazu gehören Fragen des Datenschutzes, der informierten Einwilligung der spendenden Person und die Sicherheit der Daten. Die zukünftige Entwicklung wird stark von der regulatorischen Umgebung, technologischen Fortschritten und der Akzeptanz in der Bevölkerung abhängen. Die Datenspende im Gesundheitsbereich steht erst am Anfang ihrer rechtlichen Entwicklung. Mit dem Fortschritt in der Technologie und der zunehmenden Digitalisierung des Gesundheitswesens wird erwartet, dass die Datenspende eine immer wichtigere Rolle in der medizinischen Forschung und Patientenversorgung spielen wird.<sup>47</sup> Dies erfordert eine kontinuierliche Anpassung und Präzisierung der rechtlichen Rahmenbedingungen, um den Schutz der Individuen

---

<sup>60</sup> Staab, P. (2019). *Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit*. Berlin: Suhrkamp.

<sup>61</sup> Dolata, U. & Schrape, J.-F. (2022). Plattform-Architekturen. *KZfSS - Kölner Zeitschrift für Soziologie und Sozialpsychologie*, 74, 11–34.

<sup>62</sup> Süß, A., Wulf, N. & Betz, S. (2021). Technologische Grundlagen eines PAYL-Systems - Der Elefant im Raum – wie steht es mit dem Datenschutz und der IT-Sicherheit? *Zugluft – Öffentliche Wissenschaft in Forschung, Lehre und Gesellschaft*, 2, 50-55. <https://www.prointernet.de/Blaetterkatalog/Zugluft/02/>

<sup>63</sup> Acquisti, A., Brandimarte, L. & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, 30, 736-758. <https://doi.org/10.1002/jcpy.1191>

<sup>64</sup> Petersen, A. (2019). *Digital Health and Technological Promise: A Sociological Inquiry*. London: Routledge.

<sup>65</sup> Nolte, D. (2021). Vom Datengrab zum Datenschatz? Strukturierte Behandlungsprogramme (Disease Management Programme) für chronisch Kranke – ein Praxisbeispiel für digitale Datensammlung im Gesundheitswesen. *Zugluft – Öffentliche Wissenschaft in Forschung, Lehre und Gesellschaft*, 2, 82-87. <https://www.prointernet.de/Blaetterkatalog/Zugluft/02/>

und die Förderung der Forschung gleichermaßen zu gewährleisten. Gleichzeitig gilt es, diese rechtlichen Aspekte mit ethischen und datenschutzrechtlichen Überlegungen sorgfältig abzuwägen. Mit dem richtigen Rahmenwerk versehen, ist davon auszugehen, dass die Datenspende zu bedeutenden Fortschritten im Gesundheitssektor beitragen kann.

## **Acknowledgement**

Wir bedanken uns bei Julia Berghäuser für die Koordination dieses Beitrags und die redaktionelle Unterstützung bei der Manuskripterstellung.