Virtuelle Zwillinge und Diabetes

David M. Schneeberger[*]

A. Einleitung

Diabetes betrifft einen von zehn Erwachsenen weltweit und führte 2021 zu 6,7 Millionen Todesfällen. Im selben Jahr erzeugte die Krankheit mindestens 966 Milliarden Dollar an Gesundheitsausgaben.[1] Diabetes ist damit ein Problem, das die gesamte Gesellschaft, verstärkt jedoch ärmere Länder, betrifft. Eine personalisierte Behandlung, die mit dem verbreiteten one-size-fits-all-Ansatz bricht, könnte den Behandlungserfolg verbessern. An diesem Schnittpunkt trifft das Metaversum auf die Medizin. So lässt sich die physische Welt, bspw. Körperbestandteile oder ganze Patienten, digital bzw. dreidimensional nachbilden.[2] Eine solche „Nachbildung" wird als „virtueller" bzw. „digitaler Zwilling" bezeichnet.[3] Anhand dieser virtuellen Abbildungen können Therapien erprobt und Änderungen beobachtet werden. Auf europäischer Ebene wird dieser Ansatz bspw. durch das European-Virtual-Human-Twin-Projekt (EDITH) verfolgt.[4]

Diesem Ziel, den Behandlungserfolg durch Rückgriff auf virtuelle Zwillings-Modelle zu steigern, hat sich auch das dAIbetes-Projekt verschrieben. Dieser Beitrag gibt einen Überblick über erste Rechtsfragen, die im Zuge des Anfang 2024 begonnenen Projektes aufgeworfen wurden. Er behandelt nach einer kurzen Vorstellung des Projektes (B.) ausgewählte rechtliche Aspekte, darunter Fragen des Datenschutzrechtes (C.), insb. der gemeinsamen Verantwortlichkeit, von Synergien und Friktionen zwischen Medi-

* Dieser Beitrag wurde durch das Projekt „dAIbetes – Prediction of treatment outcome in type 2 diabetes" (Horizon Europe Research and Innovation Programme Grant Agreement no. 101136305) gefördert.

1 *IDF*, IDF Diabetes Atlas, diabetesatlas.org/ (abgerufen am 13.12.2024).

2 *T. Meier*, Medizinprodukte für das Metaverse, MPR 2022, 134 (137).

3 *R. Laubenbacher/B. Mehrad/I. Shmulevich/N. Trayanova*, Digital twins in medicine, nature computational science 2024, 184 (184).

4 *EDITH*, edith-csa.eu/edith/ (abgerufen am 13.12.2024).

zinprodukteverordnung (MPVO)[5] und der Verordnung über Künstliche Intelligenz (KI-VO)[6] (D.) und des Cybersicherheitsrechtes (E.). Eine abschließende Conclusio (F.) präsentiert die wichtigsten Ergebnisse.

B. Das dAIbetes-Projekt

I. Einleitung

Ein großes Problem beim Trainieren von Machine-Learning-Modellen im Gesundheitsbereich liegt im Mangel an hochqualitativen Trainingsdaten. Selbst wenn diese existieren, liegen sie oft verstreut innerhalb und außerhalb von Europa vor. Eine Zusammenfügung dieser großen Mengen äußerst sensibler personenbezogener Daten wirft häufig (datenschutz-)rechtliche[7] und ethische[8] Fragen auf.

Als Lösungsansatz hat sich das dAIbetes-Projekt das Ziel gesetzt, federated (machine) learning zu verwenden, um eine Gesundheitsdatenplattform zu errichten, die das rechtssichere Training von virtuellen Zwillings-Modellen für Typ 2 Diabetes ermöglicht. Durch die Integration von Big Data (ca. 800 000 Patientendaten) soll im Sinne der personalisierten Medizin eine bessere Prädiktion des Behandlungserfolges ermöglicht werden.[9]

Die Patientendaten werden dabei von sechs klinischen Partnern, wobei fünf in Europa angesiedelt sind, bereitgestellt. Als amerikanischer Partner ist ein Partner (im Folgenden Partner 1) als klinischer Partner und Leiter des Arbeitspaketes Datenharmonisierung beteiligt.[10] Diese europäisch-ame-

5 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) 178/2002 und der Verordnung (EG) 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (Medizinprodukteverordnung), ABl. L 2017/117, 1.

6 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L 2024/144, 1.

7 Statt vieler *D. Linardatos*, Intelligente Medizinprodukte und Datenschutz (Teil 1), CR 2022, 367.

8 *G. Rubeis*, Ethics of Medical AI, Cham 2024, S. 91 ff.

9 dAIbetes, daibetes.eu/ (abgerufen am 13.12.2024).

10 Work packages, daibetes.eu/teams-partnes/work-packages (abgerufen am 13.12.2024).

rikanische Zusammenarbeit wirft komplexe Rechtsfragen des Anwendungsbereiches von Europarecht auf, die auch auf andere Konstellationen übertragbar sein könnten.

Das Projekt beinhaltet eine abschließende Validierungsstudie, mit der die eingesetzten virtuellen Zwillinge evaluiert werden sollen. Die Studie ist dabei so konzipiert, dass die Ergebnisse des Modells die Behandlung nicht beeinflussen, da das Gesundheitspersonal dafür „blind" ist, d.h. nicht über das Ergebnis informiert wird. Die Validierungsstudie wird vom zweiten amerikanischen Partner (im Folgenden Partner 2) geleitet.[11]

II. Federated learning

Ein Kernelement des Projektes ist federated learning. Beim federated learning werden, anstatt alle Daten von verschiedenen Standorten auf einem zentralen Server zu „poolen", von den Beteiligten dezentrale (sog. lokale) Modelle trainiert, die daraufhin vom sog. „Koordinator" aggregiert und zu einem globalen Modell zusammengefügt werden. Dieses wird wiederum den Beteiligten zur Verfügung gestellt.[12]

Vorteil ist, dass nicht die (personenbezogenen) Daten, sondern nur die Parameter der Modelle ausgetauscht werden. Die Patientendaten verlassen damit nicht den jeweiligen Beteiligten (z.B. die Krankenanstalt).[13] Da zwischen den aggregierten Daten und den konkreten Patienten keine „Verbin-

11 Work packages, daibetes.eu/teams-partnes/work-packages (abgerufen am 13.12.2024).

12 *J. Baumbach/M. M. K. Majdabadi/C. C. Saak/M. Bakhtiari/N. Probul*, Föderiertes Lernen, in: G. Buchholtz/L. Hering (Hrsg.), Digital Health und Recht, Berlin 2024, S. 263 (264 ff.); *X. Lareo*, Federated Learning, edps.europa.eu/press-publications/publications/techsonar/federated-learning_en (abgerufen am 13.12.2024). Der federated-learning-Ansatz wurde bereits im Vorgängerprojekt FeatureCloud auf seine Tauglichkeit für (bio-)medizinische Anwendungen erprobt, *Baumbach/Majdabadi/Saak/Bakhtiari/Probul,* Lernen (Fn. 12), S. 280 ff.; J. *Matschinske/J. Späth/M. M. Bakhtiari/N. Probul/M. M. K. Majdabadi/R. Nasirigerdeh/R. Torkzadehmahani/A. Hartebrodt/B.-A. Orban/S.-J. Fejér/O. Zolotareva/S. Das/L. Baumbach/J. K. Pauling/O. Tomašević/B. Bihari/M. Bloice/N. C. Donner/W. Fdhila/T. Frisch/A.-C. Hauschild/D. Heider/A. Holzinger/W. Hötzendorfer/J. Hospes/T. Kacprowski/M. Kastelitz/M. List/R. Mayer/M. Moga/H. Müller/A. Pustozerova/R. Röttger/C. C. Saak/A. Saranti/H. H. H. W. Schmidt/C. Tschohl/N. K. Wenke/J. Baumbach*, The FeatureCloud Platform for Federated Learning in Biomedicine, Journal of medical Internet research 2023, e42621.

13 *A. Brauneck/L. Schmalhorst/M. M. K. Majdabadi/M. Bakhtiari/U. Völker/J. Baumbach/L. Baumbach/G. Buchholtz*, Federated Machine Learning, Privacy-Enhancing

dungslinie“ mehr gezogen werden kann, ist der Anwendungsbereich der DSGVO[14] – wenn zusätzliche Schutzmaßnahmen getroffen werden – in Bezug auf die Modelle ausgeschlossen.[15]

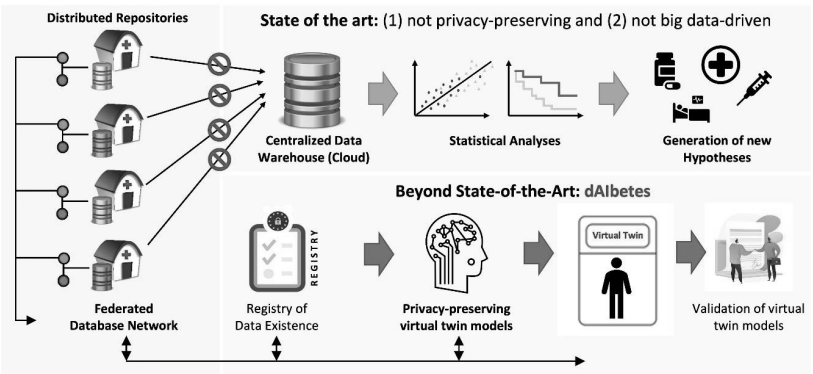

Abbildung 1 dAIbetes Projekt-Visions-Diagramm (daibetes.eu/as-a-whole)

III. Virtuelle Zwillinge

Ein Hinweis zu Beginn: Derzeit besteht keine Einigkeit über den Begriff „virtueller Zwilling“, der als Bezeichnung für einfache Modelle bis hin zu vollen digitalen Abbildungen von Patienten, die kontinuierlich oder periodisch aktualisiert werden, verwendet wird.[16]

Die European Virtual Human Twins Initiative schlägt bspw. folgende Definition vor: „A virtual human twin (VHT) is a digital representation

Technologies, and Data Protection Laws in Medical Research, Journal of medical Internet research 2023, 1 (3 f.).

14 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 2016/119, 1.

15 *D. Linardatos*, Intelligente Medizinprodukte und Datenschutz (Teil 2), CR 2022, 571 (574).

16 *Laubenbacher/Mehrad/Shmulevich/Trayanova*, twins (Fn. 3), 185; vgl. *L. Wright/S. Davidson*, How to tell the difference between a model and a digital twin, Adv. Model. and Simul. in Eng. Sci 2020, 1. Teilweise wird auch, ohne klare Abgrenzung, der Begriff „digitale Zwillinge“ verwendet.

of a human health or disease state. They refer to different levels of human anatomy (e.g. cells, tissues, organs or organ systems)."[17]

Solche Zwillinge können die „Innenwelt" von Patienten, von Gewebe und Organen bis hin zur molekularen Struktur, abbilden.[18] Derzeit wird häufig das digitale Ebenbild einzelner Organe oder Körperteile erstellt.[19] In Zukunft sollen umfassendere virtuelle Zwillinge von individuellen Patienten möglich sein.[20]

Im Rahmen von dAIbetes wird nicht jeder Patient durch einen eigenen Zwilling repräsentiert. So soll ein Gesamtmodell – der genaue Modelltyp stand zum Zeitpunkt der Einreichung noch nicht fest – die notwendigen Zusammenhänge erfassen und personalisierte Behandlungsempfehlungen ausgeben. Als Ergebnis soll der Einfluss eines Medikaments innerhalb eines spezifischen Zeitraums auf den HbA1c-Wert, der den Blutzuckerspiegel der vorangegangenen vier bis sechs Wochen widerspiegelt,[21] herangezogen werden.[22]

C. Datenschutzrechtliche Aspekte

I. Gemeinsame Verantwortlichkeit

Federated learning wirft komplexe Fragen in Bezug auf die datenschutzrechtliche Verantwortlichkeit auf. Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO bekanntlich „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Wie der Wortlaut schon andeutet, kann diese Entscheidung auch von mehreren Verantwortlichen gemeinsam getroffen werden,

17 European Virtual Human Twins Initiative, digital-strategy.ec.europa.eu/en/policies/virtual-human-twins (abgerufen am 13.12.2024).

18 *P. Coveney/R. Highfield*, Virtual You. How Building Your Digital Twin Will Revolutionize Medicine and Change Your Life, Princeton 2023, S. 3.

19 *T. Meier*, § 27 Medizin- und Medizinprodukterecht, in H. Steege/K. Chibanguza (Hrsg.), Metaverse, Baden-Baden 2023, S. 439 (442 f.).

20 *Coveney/Highfield*, You (Fn. 18), S. 14 ff.

21 Hämoglobin A1c (HBA1C), gesundheit.gv.at/labor/laborwerte/organe-stoffwechsel/hba1c.html (abgerufen am 13.12.2024).

22 Auskunft von A. Tanzanakis, der im Rahmen von Arbeitspaket 3 unter der Leitung von B. Eskofier von der FAU Erlangen-Nürnberg maßgeblich an der Modellentwicklung beteiligt ist.

wodurch eine „gemeinsame Verantwortlichkeit" (im Englischen *joint controllership*) entsteht (Art. 26 DSGVO).[23] Konkretisierend führt der Europäische Datenschutzausschuss (EDSA) in seinen Leitlinien aus: „Das übergeordnete Kriterium für das Vorliegen gemeinsamer Verantwortlichkeit ist die gemeinsame Beteiligung von zwei oder mehr Stellen an der Festlegung der Zwecke und Mittel einer Verarbeitung."[24]

Zu Fragen der gemeinsamen Verantwortlichkeit sind inzwischen, mit zunehmender Frequenz, eine Reihe von Urteilen des EuGH ergangen, die das Konzept konkretisieren. Er vertritt ein extensives Verständnis der gemeinsamen Verantwortlichkeit.[25] So müssen gemeinsam Verantwortliche nicht zwingend den (exakt) selben Zweck verfolgen; sich ergänzende bzw. komplementäre Entscheidungen über die Zwecke und Mittel genügen.[26] Ein Verantwortlicher kann auch mehr Einfluss haben als ein anderer.[27] Bereits wenn ein Beteiligter die Mittel (z.B. die Nutzung einer Plattform) definiert und diese von den anderen Beteiligten angenommen werden, kann eine gemeinsame Verantwortlichkeit vorliegen.[28] Ein marginaler Einfluss auf die Mittel kann ausreichen.[29] Dabei indiziert ein „Eigeninteresse", dass es sich um eine gemeinsame Verantwortlichkeit handelt.[30] Dieses liegt jedoch in

23 M.w.N. *J. Marosi*, (Gem-)Einsame Verantwortlichkeit im Datenschutzrecht. Voraussetzungen, Folgen, Perspektiven, Trier 2024, S. 179 ff.; *T. Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO. Unter besonderer Berücksichtigung von Internetsachverhalten, Baden-Baden 2021, S. 45 ff.; *R. Schneider*, Gemeinsame Verantwortlichkeit. Entstehung, Ausgestaltung und Rechtsfolgen des Innenverhältnisses gemäß Art. 26 DSGVO, Wiesbaden 2021, S. 34 ff.

24 *EDSA*, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO Version 2.0, 2021, S. 22, edpb.europa.eu/system/files/2023–10/edpb_guidelines_202007_controllerprocessor_final_de.pdf.

25 *C. Millard*, At this rate, everyone will be a [joint] controller of personal data! IDPL 2019, 217.

26 *V. Halim/J. Marosi*, Status Quo der EuGH-Rechtsprechung zu Personenbezug und gemeinsamer Verantwortlichkeit, CR 2024, 297 (303); *J. Hartung* in: J. Kühling/B. Buchner (Hrsg.), DS-GVO/BDSG. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 4. Auflage, München 2024, Art. 26 DSGVO Rn. 17; *J. Marosi*, Halbherzig beauftragt ist gemeinsam verantwortet, DSB 2024, 46 (47).

27 *J. Dumortier/P. Gryffroy* in: I. Spiecker gen. Döhmann/V. Papakonstantinou/G. Hornung/P. Hert (Hrsg.), General Data Protection Regulation. Article-by-Article Commentary, Baden-Baden/München/Oxford 2023, Art. 26 GDPR Rn. 37.

28 *K.-U. Plath* in: K.-U. Plath (Hrsg.), DSGVO/BDSG/TTDSG. Kommentar, 4. Auflage, Köln 2023, Art. 26 DSGVO Rn. 11.

29 *M. Finck*, Cobwebs of control, IDPL 2021, 333 (335).

30 EuGH C-683/21, *Nacionalinis visuomenės sveikatos centras,* ECLI:EU:C:2023:949 Rn. 43; *Halim/Marosi,* Status Quo (Fn. 26), 304; *Marosi,* Halbherzig (Fn. 26), 46.

Projekten typischerweise bei allen Partnern vor, die gemeinsam, bspw. im Steering Committee, grundlegende Entscheidungen treffen.[31] So werden in der Literatur bereits die gemeinsame Nutzung der Ergebnisse eines Projektes und gemeinsame IP-Rechte als Indikatoren für eine gemeinsame Verantwortlichkeit gewertet.[32] Um das extensive Ausmaß einer gemeinsamen Verantwortlichkeit in Projekten wieder zurückzudrängen, wurden bspw. „Filtermodelle" vorgeschlagen.[33] Als wichtiger Punkt ist es nicht notwendig, dass jeder Verantwortliche Zugang zu den Daten hat.[34] So reichte die Organisation von Verkündigungstätigkeiten durch eine Religionsgemeinschaft – die keinen Zugriff auf die Daten hatte – zur Qualifizierung als gemeinsam Verantwortlicher aus.[35] Auch der Einfluss auf die Entwicklung einer COVID-19-Tracking-App und die dafür vorgesehene Verarbeitung durch Bestimmung der Parameter führte zur Einstufung als gemeinsam Verantwortlicher.[36]

Aufgrund der dargestellten extensiven Rspr. erscheint es prima facie naheliegend, dass das gesamte dAIbetes-Konsortium – da es gemeinsam über die Zwecke (Verbesserung der Diabetes-Behandlung) und Mittel (z.B. Training föderierter virtueller Zwillinge) entscheidet – einer gemeinsamen Verantwortlichkeit in Bezug auf den Aufbau der Infrastruktur (*federated database network*), das Training der virtuellen Zwillinge und die Validierungsstudie unterliegt.

II. Anwendungsbereich der DSGVO

1. Einleitung

Mit Verweis auf die obigen Ausführungen zur gemeinsamen Verantwortlichkeit ergibt sich in Hinblick auf die Anwendbarkeit der DSGVO auf

31 *E.-B. Veen/M. Boeckhout/I. Schlünder/J. W. Boiten/V. Dias*, Joint controllers in large research consortia, Open Res Europe 2024, 1 (5), https://doi.org/10.12688/openreseurope.14825.2.

32 *R. Becker/A. Thorogood/J. Bovenberg/C. Mitchell/A. Hall*, Applying GDPR roles and responsibilities to scientific data sharing, IDPL 2022, 207 (216).

33 *Veen/Boeckhout/Schlünder/Boiten/Dias*, controllers (Fn. 31), 8 ff.

34 EuGH C-231/22, *État belge/Autorité de protection des données,* ECLI:EU:C:2024:7 Rn. 48.

35 EuGH C-25/17, *Jehovan todistajat,* ECLI:EU:C:2018:551 Rn. 75.

36 EuGH C-683/21, *Nacionalinis visuomenės sveikatos centras,* ECLI:EU:C:2023:949 Rn. 32 ff.

die (amerikanischen) Partner ein datenschutzrechtliches „Henne-Ei-Problem", da eine gemeinsame Verantwortlichkeit, die nur bei Anwendbarkeit der DSGVO überhaupt vorliegen kann, potentiell ihre Anwendbarkeit begründet. Art. 3 DSGVO enthält drei unterschiedliche Regelungen über den räumlichen Anwendungsbereich, wobei nur zwei davon im Folgenden von Relevanz sind.

2. Niederlassungsprinzip (Art. 3 Abs. 1 DSGVO)

Nach Art. 3 Abs. 1 DSGVO findet die DSGVO zunächst „Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet." Dies trifft zunächst unstrittig auf die europäischen (klinischen) Partner zu.

Bei Annahme einer gemeinsamen Verantwortlichkeit wird in der Literatur, im Gegensatz zu einem Verantwortlichen-Auftragsverarbeiter-Verhältnis, angenommen, dass die Anwendbarkeit der DSGVO für alle Verantwortlichen gemeinsam zu beurteilen ist.[37] Dies würde auch für unionsfremde Verantwortliche gelten.[38]

Dadurch wäre im dAIbetes-Projekt, bspw. für das Training der Zwillings-Modelle, da dieses nur im Zusammenspiel mit den europäischen Partnern gelingt und von europäischen und amerikanischen Patienten abgeleitete Parameter gleichermaßen einfließen, der Anwendungsbereich der DSGVO für den amerikanischen Partner 1 eröffnet. Die Tätigkeit der europäischen Partner würde somit den Anwendungsbereich der DSGVO auch auf Partner 1, der mit diesen gemeinsam über die Zwecke und Mittel entscheidet, erstrecken.

Dies gilt auch für Leitung des Arbeitspaketes zur Datenharmonisierung durch Partner 1. Ähnlich wie die Erstellung einer Fanpage[39] bzw. die Orga-

37 *K.-W. Plath/M. A. Struck* in: K.-U. Plath (Hrsg.), DSGVO/BDSG/TTDSG. Kommentar, 4. Auflage, Köln 2023, Art. 3 DSGVO Rn. 13.

38 *S. Hanloser* in H.-A. Wolff/S. Brink/A. Ungern-Sternberg (Hrsg.), BeckOK Datenschutzrecht. DS-GVO, DA, DGA, BDSG. Datenschutz und Datennutzung, München 48. Edition, Stand: 01.11.2021, Art. 3 DSGVO Rn. 12: „In Fällen gemeinsamer Verantwortung iSd Art. 26 reicht die Unionsniederlassung eines Mitverantwortlichen, um die räumliche Anwendbarkeit der DS-GVO auch gegenüber sämtlichen unionsfremden Mitverantwortlichen zu eröffnen."

39 *Hartung* (Fn. 26), Art. 26 DSGVO Rn. 27.

nisation von Verkündigungstätigkeiten[40] die Datensammlung durch andere Verantwortliche erst ermöglichte, lässt sich dies auch für die Leitung der Datenharmonisierung, durch die die Merkmale der Modelle bestimmt werden, argumentieren.

Diese Argumentation lässt sich mit Verweis auf die aktuelle Rspr. des EuGH zu IAB Europe untermauern.[41] Der EuGH führte in dieser Entscheidung im Werbekontext aus, dass die Aufstellung eines „Regelungsrahmens" „der nicht nur verbindliche technische Vorschriften enthält, sondern auch Vorschriften, die detailliert festlegen, wie personenbezogene Daten […] gespeichert und verbreitet werden müssen," zu einer Einstufung als gemeinsamer Verantwortlicher führt, wenn die Organisation „aus Eigeninteresse auf die betreffende Verarbeitung […] Einfluss nimmt und damit gemeinsam […] die Zwecke der und die Mittel zur betreffenden Verarbeitung festlegt."[42]

Dies ähnelt der Erstellung von Vorgaben zur Datenharmonisierung durch Partner 1. Zugriff auf die Daten ist nicht notwendig. Somit würde bereits die „hintergründige Organisation und Koordination einer fremden Datenverarbeitung"[43] hinreichen. Als Zwischenfazit wäre damit die DSGVO auf Verarbeitungstätigkeiten von Partner 1 im Rahmen der gemeinsamen Verantwortlichkeit anwendbar.

Ein ähnlicher Schluss ließe sich in Hinblick auf Partner 2 ziehen. Dieser nimmt zwar nicht am Training teil, leitet jedoch die Validierungsstudie. Dabei nehmen die Leitlinien des EDSA für die gemeinsame Erstellung eines Studienprotokolls das Vorliegen einer gemeinsamen Verantwortlichkeit an.[44] Ein Vergleich zur genannten Parametrisierung einer COVID-19-Tracking-App oder die Vorgabe des Regelungsrahmens in IAB Europe liegt nahe. Damit würde auch Partner 2 im Kontext der für die Validierungsstudie notwendigen Verarbeitungen, nicht aber für andere Tätigkeiten, der DSGVO unterliegen.

Diese Interpretation von Art. 3 Abs. 1 i.V.m. Art. 26 DSGVO ist jedoch nicht unumstritten. So geht die Gesellschaft für Datenschutz und Datensicherheit (GDD) davon aus, dass, wenn der gemeinsam Verantwortliche

40 *Hartung* (Fn. 26), Art. 26 DSGVO Rn. 33 f.
41 EuGH C-604/22, *IAB Europe,* ECLI:EU:C:2024:214; vgl. *Halim/Marosi,* Status Quo (Fn. 26), 298; *V. Halim/J. Marosi*, TC-String ist ein personenbezogenes Datum, ZD 2024, 333.
42 EuGH C-604/22, *IAB Europe,* ECLI:EU:C:2024:214 Rn. 77.
43 *L. M. Keppeler/R. Schneider*, TC-String ist ein personenbezogenes Datum, MMR 2024, 395 (396).
44 *EDSA*, Verantwortlicher (Fn. 24), S. 26.

keine Niederlassung in der EU besitzt, Art. 26 DSGVO das Vorliegen der Bedingungen von Art. 3 Abs. 2 DSGVO (Marktortprinzip) erfordern würde.[45] Auch nach *Radtke* ist der Anwendungsbereich separat zu betrachten. So würde die Gemeinsamkeit der Festlegung durch einen räumlich unter die DSGVO fallenden (gemeinsam) Verantwortlichen nicht die übrigen Festlegenden „infizieren".[46]

Im Zwischenergebnis liegt eine non-liquet-Situation vor. Die Literatur lässt beide Interpretationen von Art. 3 Abs. 1 i.V.m. Art. 26 DSGVO zu. Rechtsprechung zu dieser Konstellation existiert, soweit dem Autor bekannt, bisher noch nicht. Ob es dem Telos entspricht, den Anwendungsbereich der DSGVO über das Instrument der „gemeinsamen Verantwortlichkeit" über die EU hinaus zu erstrecken, wodurch „Daten außerhalb ihrer Grenzen"[47] geschützt werden würden, lässt sich zum derzeitigen Stand noch nicht zweifelsfrei feststellen. Eine Konkretisierung dieser zentralen Frage über aktualisierte Leitlinien des EDSA wäre, um diese Rechtsunsicherheit zu beseitigen, wünschenswert.

3. Marktortprinzip (Art. 3 Abs. 2 DSGVO)

Alternativ könnte vom Vorliegen von Art. 3 Abs. 2 lit. b DSGVO, der Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen im Kontext der Beobachtung des Verhaltens von betroffenen Personen, ausgegangen werden.

So nennen die Leitlinien in diesem Kontext auch die „Überwachung oder regelmäßige Meldungen über den Gesundheitszustand einer Person".[48] Die Erstellung eines häufig aktualisierten virtuellen Zwillings könnte solche regelmäßigen Meldungen erfordern. Ähnlich ließe sich in Bezug auf die Validierungsstudie argumentieren, dass dazu eine „Beobachtung" von Patienten notwendig sei.

---

45 *GDD*, GDD-Praxishilfe DS-GVO. Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO (Joint Controllership), 2019, S. 14, gdd.de/wp-content/uploads/2023/06/GDD-Praxishilfe-DS-GVO-Joint-Controllership.pdf.

46 *Radtke*, Verantwortlichkeit (Fn. 23), S. 161; vgl. *M. Gömann*, Das öffentlich-rechtliche Binnenkollisionsrecht der DS-GVO. Unionaler Anwendungsbereich mitgliedstaatlichen Anpassungsrechts zur Datenschutz-Grundverordnung, Tübingen 2021, S. 534 f.

47 *C. Kuner*, Protecting EU data outside EU borders under the GDPR, CMLR 2023, 77.

48 *EDSA*, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3) Version 2.0, 2019, S. 23, edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_de.pdf.

Gegen die Bejahung des Vorliegens von Art. 3 Abs. 2 DSGVO einwenden lässt sich, dass nach Projektkonzeption keine personenbezogenen Daten über europäische Patienten an die amerikanischen Partner übermittelt werden. Die Übermittlung zur Validierungsstudie erfolgt (voraussichtlich) in aggregierter und anonymisierter Form. Art. 3 Abs. 2 DSGVO hat dabei konzeptuell auch stärker „Internet-Monitoring" (ErwGr. 24 DSGVO) und nicht die Aufzeichnung von physiologischen Zuständen vor Augen.[49]

Bejaht man die These der gemeinsamen Verantwortlichkeit in Verbindung mit der Anwendbarkeit der DSGVO bedeutet dies, dass die gemeinsam Verantwortlichen im Innenverhältnis einen Vertrag, ein *joint controller agreement* (JCA) (Art. 26 Abs. 1, 2 DSGVO) abschließen müssen. Dieses hat jedoch nur deklarative, nicht aber konstitutive Wirkung. Im Außenverhältnis wird eine gesamtschuldnerische Haftung begründet (Art. 82 Abs. 4 DSGVO).[50] Wird die Anwendbarkeit der DSGVO bejaht, würden somit auch die amerikanischen Partner den Betroffenenrechten (insb. den Informationspflichten und dem Recht auf Löschung) unterliegen und müssten ein Verzeichnis der Verarbeitungstätigkeiten führen. Die praktische Durchsetzbarkeit der DSGVO in den USA wäre jedoch in dieser Konstellation – mangels einer entsprechenden Behördenstruktur – fragwürdig.

D. MPVO & KI-VO: Synergien und Friktionen

I. Virtuelle Zwillinge als Medizinprodukt

Virtuelle Zwillinge bzw. Machine-Learning-Modelle stellen eine Unterform der breiteren Kategorie „Software" dar. „Software",[51] die „dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen […] spezifischen medizinischen Zwecke erfüllen soll" kann als Medizinprodukt eingestuft werden (Art. 2 Nr. 1 MPVO). Dies lässt sich auch für dAIbetes bejahen, da als medizinischer Zweck die „Behandlung oder Linderung

49 *G. Hornung* in: I. Spiecker gen. Döhmann/V. Papakonstantinou/G. Hornung/P. Hert (Hrsg.), General Data Protection Regulation. Article-by-Article Commentary, Baden-Baden/München/Oxford 2023, Art. 3 GDPR Rn. 48.

50 *Radtke*, Verantwortlichkeit (Fn. 23), S. 228 ff.

51 *MDCG*, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, MDCG 2019–11, 2019, S. 5 f., health.ec.europa.eu/system/files/2020–09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf.

von Krankheiten" verfolgt wird. Die im Projekt vorgesehenen virtuellen Zwillinge fallen nach der – teilweise als zu streng kritisierten[52] – Klassifizierungsregel 11 (Anhang VIII Abschnitt 6.3 MPVO) mindestens in die mittlere Risikoklasse IIa, nachdem sie dazu bestimmt sind „Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden".

In Bezug auf die KI-VO führt die Einstufung als Medizinprodukt, da die verwendeten Zwillinge in Verbindung mit anderen Elementen wie der Nutzerschnittstelle als KI-Systeme[53] (Art. 3 Nr. 1 KI-VO) zu qualifizieren sein werden, prinzipiell zu einer Anwendbarkeit der KI-VO. „Intelligente Medizinprodukte" gelten, da nach MPVO ab Klasse IIa die Einbindung einer Konformitätsbewertungsstelle notwendig ist und die MPVO in Anhang I Abschnitt A KI-VO genannt wird, (großteils) gleichzeitig als Hochrisiko-KI-Systeme (Art. 6 Abs. 1 KI-VO).[54]

Im Folgenden sollen insbesondere Fragen der Interaktion zwischen den Anwendungsbereichen der MPVO und KI-VO aufgeworfen werden. Wie relevant Rechtsfragen dieser Interaktion sind, zeigt sich an den von der MDCG (Medical Device Coordination Group) angekündigten FAQ zum Zusammenhang von MPVO und KI-VO.[55]

II. Forschungsausnahme

Die KI-VO normiert eine explizite Forschungsausnahme. Diese wurde auf Anregung von Parlament und Rat eingefügt.[56] Zuvor wurde das Fehlen

52 *M. Heil*, Innovationsermöglichungsrecht oder Innovationshemmnis? in: R. Grinblat/S. Scholtz/S. Stock (Hrsg.), Medizinprodukterecht im Wandel. Festschrift für Ulrich M. Gassner zum 65. Geburtstag, Baden-Baden 2022, S. 447 (454).

53 *C. Wendehorst/B. Nessler/A. Aufreiter/G. Aichinger*, Der Begriff des „KI-Systems" unter der neuen KI-VO, MMR 2024, 605.

54 *M. Martini*, § 4. Hochrisiko-KI-Systeme, in: E. Hilgendorf/D. Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, München 2023, S. 51 (65 f.); *R. Schwartmann/E.-M. Pottkämper*, Hochrisiko-KI-Systeme gem. Art. 6 Abs. 1 KI-VO (Anhang I), in R. Schwartmann/T. O. Keber/K. Zenner (Hrsg.), KI-Verordnung. Leitfaden für die Praxis, Heidelberg 2024, S. 79 (80).

55 *MDCG*, Ongoing/planned guidance development and deliverables of MDCG Subgroups – March 2024, 2024, S. 4, health.ec.europa.eu/document/download/f588a5c8–57af-48aa-808f-1d9c02f4925a_en?filename=mdcg_ongoing-guidance_0.pdf.

56 *T. O. Keber/K. Zenner*, Forschung, in R. Schwartmann/T. O. Keber/K. Zenner (Hrsg.), KI-Verordnung. Leitfaden für die Praxis, Heidelberg 2024, S. 47 (48).

einer solchen Ausnahme[57] bzw. die fehlende Abstimmung zwischen MPVO und KI-VO[58] kritisiert. Nach Art. 2 Abs. 6 KI-VO gilt die Verordnung nicht „für KI-Systeme oder KI-Modelle, einschließlich ihrer Ausgabe, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden." Der Begriff Forschung ist weit zu verstehen und bezieht sich auf eine beliebige Forschungs- und Entwicklungstätigkeit, die sich auch nicht gerade auf KI-Systeme selbst beziehen muss.[59] Forschung erfasst begrifflich sowohl Forschende in privaten Unternehmen als auch bei öffentlichen Stellen.[60] Im Rahmen der Projektphase, die der Erforschung der Anwendbarkeit von federated learning und virtuellen Zwillingen auf die komplexe Erkrankung Diabetes dient – nicht aber in Bezug auf eine eventuelle spätere Vermarktung – lässt sich insofern argumentieren, dass diese durch die Forschungsausnahme nicht dem Anwendungsbereich der KI-VO unterliegt.

Im Gegensatz zur KI-VO kennt die MPVO keine eindeutige Forschungsausnahme.[61] Zwar wird das (zukünftige) Produkt im Rahmen der Projektphase nicht in Verkehr gebracht, aber es könnte eine Inbetriebnahme durch die klinischen Partner vorliegen. Inbetriebnahme bezeichnet den Zeitpunkt, zu dem ein Produkt dem Endanwender als ein Erzeugnis zur Verfügung gestellt wird, das erstmals als gebrauchsfertiges Produkt entsprechend seiner Zweckbestimmung auf dem Unionsmarkt verwendet werden kann (Art. 2 Nr. 29 MPVO). Bereits Produkte, die in Gesundheitseinrichtungen hergestellt und verwendet werden, gelten als in Betrieb genommen (Art. 5 Abs. 4 MPVO).

Daher kommt es potentiell zu einem Auseinanderfallen zwischen den Rechtsmaterien, bei denen die Zwillinge im Rahmen der Forschungsaus-

57 *D. Feuerstack/D. Becker/N. Hertz*, Die Entwürfe des EU-Parlaments und der EU-Kommission für eine KI-Verordnung im Vergleich, ZfDR 2023, 421 (432); *N. A. Schmuha/E. Ahmed-Rengers/A. Harkens/W. Li/J. MacLaren/R. Piselli/K. Yeung*, How the EU Can Achieve Legally Trustworthy AI. A Response to the European Commission's Proposal for an Artificial Intelligence Act, 2021, S. 15 ff., papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991.

58 *Heil*, Innovationsermöglichungsrecht (Fn. 52), S. 459.

59 *C. Wendehorst* in: M. Martini/C. Wendehorst (Hrsg.), KI-VO, München 2024, Art. 2 KI-VO Rn. 83 f.

60 *Keber/Zenner*, Forschung (Fn. 56), S. 48.

61 Zur (abweichenden) Kategorie der Research-Use-Only-Produkte, siehe *MDCG*, Guidance on the health institution exemption under Article 5(5) of Regulation (EU) 2017/745 and Regulation (EU) 2017/746, MDCG 2023–1, 2023, S. 6, health.ec.europa.eu/system/files/2023–01/mdcg_2023–1_en.pdf.

nahme nicht der KI-VO unterliegen, der Anwendungsbereich der MPVO aber nicht ausdrücklich ausgeschlossen ist. Jedoch lässt sich argumentieren, dass, da die Ergebnisse des Modells auch im Rahmen der Validierungsstudie keinen Einfluss auf die Behandlung haben, keine Verwendung eines gebrauchsfertigen Produktes „entsprechend der Zweckbestimmung" und damit keine Inbetriebnahme i.e.S. vorliegt. Auch bei einem anderen Design der Studie wären die Modelle potentiell als „Prüfprodukte", d.h. ein Produkt, das im Rahmen einer klinischen Studie bewertet wird (Art. 2 Nr. 46 MPVO) einzustufen. Für Prüfprodukte bestehen wiederum Ausnahmen vom Anwendungsbereich (Art. 2 Nr. 27–29 MPVO). Faktisch dürften sich diese Überlegungen dadurch relativieren, dass die Anforderungen von KI-VO und MPVO stets mitbedacht werden sollten, wenn die Intention besteht, ein KI-System bzw. eine Software später in Verkehr zu bringen. Denn selbst wenn für die Projektphase eine Ausnahme oder Erleichterung besteht, haben die Anforderungen der Verordnungen gravierenden Einfluss auf das Design und können somit häufig nicht nachträglich berücksichtigt werden.

Eine alternative Möglichkeit wäre das Stützen auf die Ausnahme zur „Prototyp-Entwicklung", die der Markteinführung zeitlich vorausgeht (Art. 2 Abs. 8 KI-VO).[62] Diese Ausnahme stellt stärker als die Forschungsausnahme auf Tätigkeiten in Bezug auf KI-Systeme selbst ab.[63] Allerdings fallen Tests unter Realbedingungen (Art. 60 KI-VO), d.h. der befristete Test eines KI-Systems auf seine Zweckbestimmung, der unter Realbedingungen außerhalb eines Labors oder einer anderweitig simulierten Umgebung erfolgt (Art. 3 Nr. 57 KI-VO), nicht unter diesen Ausschluss. Diese müssen im Einklang mit geltendem Unionsrecht – bspw. Anforderungen an klinische Studien – durchgeführt werden.[64] Solche Tests unter Realbedingungen – die eine gewisse thematische Verwandtschaft zu Prüfprodukten nach der MPVO aufweisen – dürften in Bezug auf medizinische Anwendungen häufig notwendig sein, wodurch die Ausnahme diesbezüglich nur geringere Relevanz aufweist.

62 *J. Wendt/D. H. Wendt*, Das neue Recht der Künstlichen Intelligenz. Artificial Intelligence Act (AI Act), Baden-Baden 2024, S. 54.
63 *Wendehorst* (Fn. 59), Art. 2 KI-VO Rn. 89.
64 *Wendehorst* (Fn. 59), Art. 2 KI-VO Rn. 92.

III. „Eigenherstellung"

In Bezug auf federated learning stellen sich in Hinblick auf die „in-house"-Ausnahme bzw. „Eigenherstellung" komplexe Fragen des Anwendungsbereiches der MPVO. So wäre bspw. vorstellbar, dass die dAIbetes-Zwillinge nach Ende der Projektphase durch die klinischen Partner in praktische Verwendung übergehen bzw. in beteiligten Krankenanstalten in Betrieb genommen, aber nicht allgemein über diese hinaus in Verkehr gebracht werden.

Für Medizinprodukte, „die ausschließlich innerhalb von in der Union ansässigen Gesundheitseinrichtungen hergestellt[65] und verwendet werden" gelten gem Art. 5 Abs. 5 MPVO die Anforderungen der Verordnung – mit Ausnahme der grundlegenden Sicherheits- und Leistungsanforderungen – nicht, wenn eine Reihe von Bedingungen erfüllt werden. Für diese Produkte in „Eigenherstellung" entfällt die Pflicht zur Durchführung eines Konformitätsbewertungsverfahrens und der Anbringung der CE-Kennzeichnung.[66] Durch diese Erleichterung sollte Gesundheitseinrichtungen die Möglichkeit eingeräumt werden, Produkte hausintern herzustellen, um auf spezifische Bedürfnisse von Patienten einzugehen, die auf dem angezeigten Leistungsniveau nicht durch ein gleichartiges, auf dem Markt befindliches Produkt, befriedigt werden können.[67]

Bedingungen sind dabei u.a. eine entsprechende Dokumentation, die Bereitstellung von Informationen an Behörden und die Einhaltung von Qualitätsmanagementsystemen.[68] Dabei muss begründet werden, dass die spezifischen Erfordernisse der Zielgruppe nicht bzw. nicht auf dem Leistungsniveau durch ein auf dem Markt befindliches gleichartiges Produkt befriedigt werden können.[69] Dieses Kriterium kann potentiell in Hinblick auf die dAIbetes-Modelle, im Projekt bestehen hohe Performanz-Ziele, und Diabetes-Patienten als Zielgruppe, bejaht werden. Eine weitere Bedingung bezieht sich darauf, dass das Produkt nicht an eine andere rechtlich eigen-

65 Nach den Leitlinien kann der Begriff „herstellen" auch im Sinne einer Kombination von Produkten oder Modifikation verstanden werden, *MDCG*, health institution exemption (Fn. 61), S. 5 f.

66 *S. A. Wagner* in: W. A. Rehmann/S. A. Wagner (Hrsg.), MP-VO, 4. Auflage, München 2023, Art. 5 MPVO Rn. 45.

67 *Wagner* (Fn. 66), Art. 5 MPVO Rn. 45.

68 *MDCG*, health institution exemption (Fn. 61), S. 8 ff.

69 *MDCG*, health institution exemption (Fn. 61), S. 12 f.

ständige Einrichtung abgegeben wird.[70] In Bezug auf die lokalen Modelle lässt sich argumentieren, dass diese ausschließlich anhand der eigenen Daten trainiert und damit innerhalb von in der Union ansässigen Gesundheitseinrichtungen hergestellt und verwendet werden.

Komplexere Fragen stellen sich aufgrund des Zusammenspiels von verschiedenen Partnern in Bezug auf federated learning. Zwar wird bei der Aggregierung nicht das gesamte Modell „abgegeben", sondern nur gewisse Parameter, die zum globalen Modell zusammengefügt und wieder an die Beteiligten verteilt werden. Dieser Vorgang der Beteiligung anderer klinischer Partner und der Aggregierung führt jedoch dazu, dass m.E. nicht mehr von einer Eigenherstellung gesprochen werden kann. Eine Ausnahme könnte bei federated learning innerhalb von mehreren Krankenanstalten, die rechtlich zu einem Träger gehören,[71] vorliegen, da somit keine „Abgabe" an eine rechtlich eigenständige Einrichtung vorliegen würde. Dieser Schluss, dass federated learning der Erleichterung durch „Eigenherstellung" konzeptuell entgegensteht, DSGVO und MPVO somit Friktionen aufweisen, wird für dAIbetes dadurch bestärkt, dass das globale Modell an den amerikanischen Partner 1 abgegeben wird. Es ist somit definitionsmäßig kein Produkt, das in „ausschließlich innerhalb von in der Union ansässigen Gesundheitseinrichtungen hergestellt und verwendet" wird.

IV. Kontinuierlich lernende Medizinprodukte

Eine regulatorische Einschränkung, die generell in Bezug auf „intelligente Medizinprodukte" vorliegt, die aber gerade in Hinblick auf die dezentrale Natur von federated learning und die Möglichkeit, neue klinische Partner hinzuzufügen, verstärkt Relevanz erlangen könnte, ist die bisher eingeschränkte Möglichkeit, kontinuierlich lernende Medizinprodukte zu zertifizieren.[72]

70 *C. Johner*, Eigenherstellung von Medizinprodukten, johner-institut.de/blog/regulatory-affairs/eigenherstellung-von-medizinprodukten/ (Stand 24.10.2019).

71 *MDCG*, health institution exemption (Fn. 61), S. 8.

72 *IG-NB*, Questionnaire „Artificial Intelligence (AI) in medical devices", Version 4 2022, S. 4, ig-nb.de/veroeffentlichungen: "Dynamic AI (AI that continues to learn in the field) is not certifiable in principle, as the system must be verified and validated (among other things, the functionality must be validated against the intended use)." Statt vieler *Heil*, Innovationsermöglichungsrecht (Fn. 52), S. 462 f.; *J. L. Saliba*, Arzneimittel und Medizinprodukte, in K. Chibanguza/C. Kuß/H. Steege (Hrsg.),

Wären die dAIbetes-Zwillinge als Medizinprodukt in ihrer Konformität zertifiziert (Art. 52 MPVO) und würde sich ein zusätzlicher klinischer Partner am federated learning beteiligen wollen, würde eine (wesentliche) Änderung am Modell zum derzeitigen Stand einen erneuten Durchlauf des Konformitätsbewertungsverfahrens erfordern. Dies ist in Hinblick auf die Sicherheit des Medizinproduktes verständlich, steht einer raschen Anpassung jedoch entgegen. Das Idealbild von virtuellen Zwillingen sieht aber gerade eine solche ständige Wechselbeziehung zwischen realem Patienten und Zwilling vor. Diesbezüglich ist aber aufgrund der in der KI-VO vorgesehenen Möglichkeit, Änderungen – die damit keine erneute Konformitätsbewertung erfordern – vorab festzulegen und zu dokumentieren (Art. 43 Abs. 4 KI-VO), Anpassungen in Leitlinien[73] und zunehmend lauter werdenden Stimmen in der Literatur zu „antizipierten Konformitätsbewertungen"[74] davon auszugehen, dass es zu einer Richtungsänderung und Angleichung zwischen MPVO und KI-VO kommen wird.

E. Cybersicherheit

I. Einleitung

Auch wenn federated learning datenschutzrechtlich zahlreiche Vorteile mit sich bringt, stellt sich die Frage nach der Cybersicherheit dieser Systeme. Zwar wird durch diesen Ansatz das Risiko von Cyberangriffen verringert, dennoch sind eine Reihe von Attacken, bspw. auf die lokalen und globalen Modelle, möglich.[75]

Künstliche Intelligenz. Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden 2022, S. 627 (635 f.).

73 *IG-NB*, Questionnaire „Artificial Intelligence (AI) in medical devices", Version 5.1 2024, S. 5, ig-nb.de/veroeffentlichungen.

74 *Z. Schreitmüller*, Regulierung intelligenter Medizinprodukte. Eine Analyse unter besonderer Berücksichtigung der MPVO und DSGVO, Baden-Baden 2023, S. 153 f.; vgl. *S. Semmler/K. Stöger*, Rechtsfragen rund um eHealth, JMG 2024, 192 (201); *U. Gassner/U. Juknat*, Künstliche Intelligenz in der Medizin, in: W. A. Rehmann/C. Tillmanns (Hrsg.), E-Health/Digital Health, München 2022, S. 240 (267 ff.).

75 *Baumbach/Majdabadi/Saak/Bakhtiari/Probul,* Lernen (Fn. 12), S. 273 f.

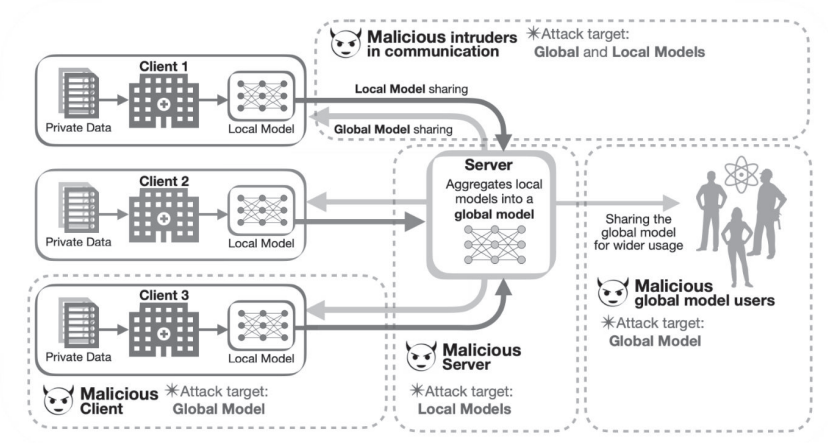

Abbildung 2 Angriffsvektoren bei federated learning (SBA Research)

Mögliche „Angriffsvektoren" bestehen bspw. auf Seite der klinischen Partner, die lokale Modelle trainieren, beim Koordinator, der das globale Modell aggregiert, in der Kommunikation zwischen Partnern und Koordinator sowie auf der Seite der Nutzer des globalen Modells.

II. Datensicherheit

Cybersicherheitsrecht stellt häufig eine Gemengelage aus unterschiedlichen Rechtsmaterien dar. Dabei unterliegen Verantwortliche bereits aufgrund der DSGVO der Pflicht, geeignete technische und organisatorische Maßnahmen (TOMs) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Dies dient u.a. der Integrität, Verfügbarkeit und Vertraulichkeit personenbezogener Daten.[76]

76 *P. Vogel*, Künstliche Intelligenz und Cybersicherheitsrecht im Krankenhaus, in: T. Dittrich/C. Dochow/J. Ippach (Hrsg.), Rechtshandbuch Cybersicherheit im Gesundheitswesen, Heidelberg 2024, S. 339 (342 f.).

III. Art. 15 KI-VO

Speziell in Bezug auf KI-Systeme verlangt Art. 15 Abs. 1 KI-VO neben Anforderungen an Genauigkeit und Robustheit ein ausreichendes Maß an Cybersicherheit. So müssen Hochrisiko-KI-Systeme widerstandsfähig gegen Versuche unbefugter Dritter sein, ihre Verwendung, Ausgaben oder Leistung durch Ausnutzung von Systemschwachstellen zu verändern (Art. 15 Abs. 5 KI-VO).[77] Das Risiko in Bezug auf die Cybersicherheit fließt dabei auch in die Bewertung im Rahmen des einzurichtenden Risikomanagementsystems (Art. 9 KI-VO) ein.[78]

Die KI-VO nennt dabei beispielhaft die Implementierung von Maßnahmen gegen data poisoning, model poisoning, adversarial examples und model evasions, Angriffe auf vertrauliche Daten oder Modellmängel.[79] Ähnliche Angriffsvektoren, z.B. model poisoning der lokalen Modelle,[80] wurden auch in Bezug auf federated learning identifiziert und müssen somit durch technische Maßnahmen verhindert werden.

IV. NIS-2-RL

Neben der KI-VO ist in Zukunft die NIS-2-RL[81] und ihre nationale Umsetzung zu beachten. Für das dAIbetes-Projekt von Relevanz designiert diese das Gesundheitswesen als Sektor mit hoher Kritikalität (Anhang I Nr. 5). Darunter fallen Gesundheitsdienstleister, d.h. eine natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines

77 *C. Glugla*, Cybersicherheit in der KI-Verordnung, RDI 2024, 421.

78 M.w.N. *D. M. Schneeberger/W. Hötzendorfer/C. Tschohl* in: C. N. Pehlivan/N. Forgó/P. Valcke (Hrsg.), The EU Artificial Intelligence (AI) Act, Alphen aan den Rijn 2024, Art. 9 AI Act.

79 *P. Nägele/A. Steinbrück*, Genauigkeit, Robustheit und Cybersecurity (Art. 15 KI-VO), in R. Schwartmann/T. O. Keber/K. Zenner (Hrsg.), KI-Verordnung. Leitfaden für die Praxis, Heidelberg 2024, S. 138 (140); *Wendt/Wendt*, Recht (Fn. 62), S. 78 f.

80 *M. Martini* in: M. Martini/C. Wendehorst (Hrsg.), KI-VO, München 2024, Art. 15 KI-VO Rn. 71.

81 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 2022/333, 80.

Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt.[82] Diese Eigenschaft lässt sich für die beteiligten Krankenanstalten, abhängig von Schwellenwerten (Art. 3 Abs. 1 lit. a NIS-2-RL),[83] voraussichtlich bejahen. Zugleich fällt die Herstellung von Medizinprodukten unter die Liste der sonstigen kritischen Sektoren (Anhang II Nr. 5 NIS-2-RL).

Diese Einrichtungen unterliegen somit neben Schulungs- (Art. 20 Abs. 2 NIS-2-RL) und (mehrstufigen) Berichtspflichten (Art. 23 NIS-2-RL)[84] auch einer Pflicht, geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten (Art. 21 Abs. 1 NIS-2-RL).

V. Technische Gegenmaßnahmen

Um die angesprochenen Risiken zu minimieren und dem security-by-design-Gedanken[85] entsprechend Rechnung zu tragen, wird federated learning häufig mit anderen Techniken wie differential privacy (DP) und secure multiparty computation (SMPC) kombiniert.[86]

Bei DP wird auf kontrollierte Weise statistisches Rauschen (noise) hinzugefügt, um die Identifizierbarkeit zu verhindern.[87] Damit kann, bspw. durch Perturbation des lokalen Modells, nicht mehr nachgewiesen werden,

82 Art. 3 lit. g Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung, ABl. L 2011/88, 45.

83 *C. Monsees/M. Gehrmann*, Krankenhäuser, in: T. Dittrich/C. Dochow/J. Ippach (Hrsg.), Rechtshandbuch Cybersicherheit im Gesundheitswesen, Heidelberg 2024, S. 56 (68).

84 *Monsees/Gehrmann*, Krankenhäuser (Fn. 83), S. 75 f.

85 *Nägele/Steinbrück*, Genauigkeit (Fn. 79) S. 140.

86 *Baumbach/Majdabadi/Saak/Bakhtiari/Probul,* Lernen (Fn. 12), S. 275 ff.; *Brauneck/Schmalhorst/Majdabadi/Bakhtiari/Völker/Baumbach/Baumbach/Buchholtz*, Machine (Fn. 13), 4.

87 *J.-P. Hoepman*, Privacy is Hard and Seven Other Myths. Achieving Privacy Through Careful Design, Cambridge 2021, S. 93 ff.; *M. Kearns/A. Roth*, The Ethical Algorithm. The Science of Socially Aware Algorithm Design, New York 2020, S. 36 ff.

dass ein Patient Teil des Trainingsdatensatzes war.[88] SMPC ermöglicht es mehreren Parteien unter Nutzung von kryptographischen Verfahren (gemeinsam) Daten auszuwerten, ohne die jeweiligen Daten den Partnern gegenüber offenzulegen.[89] SMPC garantiert primär die Sicherheit des „Inputs", d.h. schützt in einem federated-learning-Szenario die lokalen Modelle.[90] Mit der Hilfe von diesen und anderen technischen Maßnahmen soll dem (Cybersicherheits-)Risiko Rechnung getragen werden, was auch im Rahmen der notwendigen Datenschutz-Folgenabschätzung Niederschlag findet.[91]

F. Conclusio

Dieser Beitrag illustrierte am Beispiel des dAIbetes-Projektes einige Problemfelder, die Fragen am Schnittpunkt von Metaversum und Medizin (-recht) aufwerfen. So kreiste der datenschutzrechtliche Abschnitt C. um die Rechtsfigur der gemeinsamen Verantwortlichkeit, die durch eine gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung entsteht, und um die zentrale Frage, ob die Regelung des Anwendungsbereiches der DSGVO in Hinblick auf dezentral organisierte, aber dennoch föderiert vernetzte Strukturen noch zeitgemäß ist, oder ob sie zu einer (nicht intendierten) Ausdehnung des Schutzes über die EU-Grenzen hinaus führt. Die zunehmende grenzüberschreitende Vernetzung und damit die zunehmende Verlagerung in das Metaversum demonstriert Rechtsunsicherheit in Bezug auf die präzise Definition der Anwendungsbereiche, die durch Leitlinien oder Rechtsprechung adressiert werden sollte.

Interaktionen und Friktionen zeigten sich auch in Hinblick auf die MPVO und KI-VO (D.). Auch hier werfen unterschiedlich ausgestaltete

88 *M. Y. Topaloglu/E. M. Morrell/S. Rajendran/U. Topaloglu*, In the Pursuit of Privacy, frontiers in Artificial Intelligence 2021, 1 (3).

89 *D. Bierbauer/L. Helminger*, Offenlegung von Daten unter Wahrung der Privatsphäre mittels SMPC (Secure Multiparty Computation), ALJ 2023, 1 (6 ff.), alj.uni-graz.at/index.php/alj/article/view/300.

90 *FeatureCloud*, Deliverable D2.4 Set of (novel) attack vectors and countermeasures. Work Package WP2 Cyber risk assessment and mitigation, 2021, S. 16 f., featurecloud.eu/wp-content/uploads/2021/12/Deliverable_D2.4_Set_of_novel_attack_vectors_and_countermeasures.pdf.

91 *FeatureCloud*, Deliverable 8.7 "Report on Data Protection Impact Assessment". Work Package 8 "Testing and evaluation in clinical translation", 2024, S. 91 ff., featurecloud.eu/wp-content/uploads/2024/01/D8.7_Report-on-Data-Protection-Impact-Assessment_FINAL_submitted.pdf.

Anwendungsbereiche und Ausnahmen, primär die Forschungsausnahme der KI-VO, die kein direktes Pendant in der MPVO hat, Fragen der Interaktion dieser eng verbundenen Rechtsmaterien auf. Auch ist federated learning datenschutzrechtlich gewollt, führt aber zu Friktionen in Hinblick auf die Erleichterung für in „Eigenherstellung" produzierte Produkte nach der MPVO. Denn die vernetzte Natur von federated learning, die eine „Abgabe" an andere Partner bedingt, steht dieser Erleichterung diametral entgegen. Ähnliches gilt für die Friktion zwischen dem Idealbild von virtuellen Zwillingen, das eine ständige Wechselbeziehung zwischen Patienten und Zwilling impliziert, und der bislang nur bedingt bestehenden Möglichkeit, kontinuierlich lernende Medizinprodukte zu zertifizieren.

Zuletzt ergeben sich bei federated learning Besonderheiten in Hinblick auf die Cybersicherheit. Abschnitt E. erläuterte die Gemengelage aus unterschiedlichen Rechtsgebieten, wobei insbesondere Art. 15 KI-VO konkrete Maßnahmen gegen Attacken auf KI-Systeme forciert. Hand in Hand gehen damit die Anforderungen der NIS-2-RL, insbesondere in Hinblick auf Risikomanagementmaßnahmen. Als technische Gegenstrategien, wobei Synergien zum Datenschutzrecht bestehen, wurden differential privacy und secure multiparty computation vorgestellt.

Das dAIbetes-Projekt ist ein Prototyp für die Anwendbarkeit von federated learning und virtuellen Zwillingen auf komplexe Krankheiten. Gelingt das Projekt, lässt sich die geschaffene Infrastruktur potentiell auch für andere Krankheiten heranziehen. Dies würde die Symbiose zwischen einer (datenschutz-)rechtssicheren Konzeption bei gleichzeitigen Fortschritten von Informatik und Medizin demonstrieren. Doch damit der intendierte Zwilling nicht zum Zerrbild wird, man denke nur an die „ungleichen" Zwillinge Schwarzenegger und DeVito im gleichnamigen Film, damit „virtual you" in der Medizin zur Realität werden kann, müssen noch eine Reihe von Friktionen am Schnittpunkt von Metaversum und Recht ausgeräumt werden.