Bundesgesundheitsbl 2024 · 67:285–291
https://doi.org/10.1007/s00103-024-03835-3
Eingegangen: 21. August 2023
Angenommen: 15. Januar 2024
Online publiziert: 8. Februar 2024


**Merle Freye**[1,2] · **Benedikt Buchner**[3]

[1] Institut für Informations-, Gesundheits- und Medizinrecht, Universität Bremen, Bremen, Deutschland
[2] Leibniz Science Campus Digital Public Health (LSC DiPH) Bremen, Bremen, Deutschland
[3] Lehrstuhl für Bürgerliches Recht, Haftungsrecht und Recht der Digitalisierung, Universität Augsburg, Augsburg, Deutschland

# Digitale Gesundheitstechnologien – das Recht als Hemmschuh oder Wegbereiter?

## Einleitung

Als empirische Wissenschaft ist die populationsbezogene Forschung in besonderem Maße auf eine umfangreiche Nutzung von Daten angewiesen. Egal ob es um die Erforschung der Bedingungen für Gesundheit und Krankheit, die Interaktion zwischen Menschen und ihrer Umwelt oder die Bewertung der Leistung von Gesundheitssystemen geht: All diese Ziele können nur erreicht werden, wenn möglichst viele Daten frei verfügbar sind, leicht verknüpft und langfristig verfolgt werden können. Erst recht gilt dieser Befund, wenn Public Health für die Gesundheitsforschung auf – regelmäßig datengetriebene – digitale Anwendungen setzt. Neben dem wohl prominentesten Beispiel für digitale Anwendungen in der Forschung – der Corona-Datenspende-App – existieren die unterschiedlichsten Studiendesigns in der Forschung *an* und *mit* digitalen Gesundheitstechnologien, die es ForscherInnen nicht nur erlauben, an Forschungsdaten zu gelangen, die „direkt aus dem Leben" der ProbandInnen stammen, sondern die auch Rekrutierungsbarrieren senken und mitunter finanzielle sowie personelle Ressourcen einsparen können [1].

Die Verarbeitung personenbezogener Gesundheitsdaten dient gleichermaßen gesundheitsbezogenen öffentlichen Interessen wie sie auch erhebliche Vorteile für den Einzelnen mit sich bringt [2]: Auf individueller Ebene geschieht dies etwa in Form einer Verbesserung von Diagnostik und Behandlung, auf übergeordneter Ebene aber auch in der Form, dass eine breite Datenbasis fundiertere gesundheitspolitische Maßnahmen gewährleistet. Dem Recht kommt dabei die Aufgabe zu, die Interessen aller beteiligten AkteurInnen in einen angemessenen Ausgleich zu bringen. Im Rahmen der populationsbezogenen Gesundheitsforschung muss das Recht einerseits für einen möglichst umfassenden Informationszugang einschließlich einer bestmöglichen Aufbereitung der Datensätze im Sinne der FAIR-Prinzipien[1] sorgen, andererseits aber auch den Persönlichkeits- und Datenschutz aller betroffenen Personen (PatientInnen, ProbandInnen, NutzerInnen etc.) gewährleisten.

Nach wie vor herrscht allerdings in der Forschungspraxis erhebliche Unsicherheit bei der Anwendung und Auslegung der einschlägigen rechtlichen Regelungen zur Verarbeitung von Forschungsdaten mittels digitaler Gesundheitstechnologien [3]. Bei Datenschutz und Forschungsfreiheit handelt es sich um 2 (Grund-)Rechte, die seit jeher in Konflikt miteinander stehen und sich nur schwer in einen Ausgleich bringen lassen [4, 5] – und noch immer wird Datenschutz in erster Linie als ein Hemmschuh für populationsbezogene Forschung wahrgenommen [6]. In diesem Diskussionsartikel wird aufgezeigt, dass allerdings mehr und mehr Lösungsansätze zu verzeichnen sind, die dem Datenschutzrecht eine forschungsfreundlichere Prägung geben, wie sie ohnehin von Anfang an in der Datenschutz-Grundverordnung (DSGVO) angelegt war. Im Folgenden werden nicht nur die Ansätze der neuen Einwilligungsmodelle, sondern auch einwilligungsfreie Lösungen und Ansätze, die den Anwendungsbereich datenschutzrechtlicher Regelungen neu definieren, beleuchtet.

## Digitale Souveränität dank Einwilligung?

Die Praxis der Forschungsdatenverarbeitung ist immer noch maßgeblich vom Primat der Einwilligung als Legitimationsgrundlage für eine Datenverarbeitung geprägt [7]. Es herrscht die Auffassung vor, dass auch zu Forschungszwecken Daten vor allem dann verarbeitet werden dürfen, wenn die Verarbeitung von einer dahingehenden Einwilligung der betroffenen Person gedeckt ist. Problematisch ist diese Wahrnehmung schon deshalb, weil die Einwilligung – obwohl an sich *die* typische Ausprägung individueller Selbstbestimmung – keineswegs gewährleisten kann, dass eine von der Einwilligung gedeckte Datenverarbeitung auch tatsächlich der autonomen

[1] FAIR-Prinzipien: Daten sollten auffindbar („findable"), zugänglich („accessible"), interoperabel („interoperable") und wiederverwendbar („reusable") sein.

Willensbildung der betroffenen Person entspricht. Dies beginnt bei der (vermeintlichen) Informiertheit der Einwilligung: Die betroffene Person soll informiert in die Verarbeitung ihrer (sensiblen Gesundheits-)Daten einwilligen, obwohl die entsprechenden Informationen regelmäßig viel zu umfangreich und kompliziert sind und häufig noch nicht einmal gelesen werden. Gerade bei digitalen Anwendungen ist die Idee der informierten Einwilligung regelmäßig auch dann wenig praxisgerecht, wenn schon aufgrund der technisch vorgegebenen Limitierungen (etwa die Displaygröße von Smartphone, Smartwatch etc.) von vornherein ausgeschlossen ist, dass die äußerst komplexen Vorgänge einer digitalen Datenverarbeitung auch nur ansatzweise über entsprechend detaillierte Informationstexte abgebildet werden können. Hinzu kommt, dass die (Forschungs-)Zwecke einer Datenverarbeitung mit Fortschreiten des Forschungsprojekts oftmals weiterentwickelt oder um neue Zwecke ergänzt werden und Informationen daher zu Beginn des Projekts gar nicht vollständig erteilt werden können.

Das Informationsmodell des deutschen und europäischen Gesetzgebers mit seinen ambitionierten Anforderungen an eine informierte Einwilligung ist somit in vielerlei Hinsicht realitätsfern. Um die informationelle Selbstbestimmung der betroffenen Personen zu gewährleisten und gleichzeitig die Interessen der Forschung im Public-Health-Bereich im Blick zu behalten, muss das Konzept der Einwilligung weiterentwickelt und es müssen auch Wege jenseits des Primats der Einwilligung als Legitimationsgrundlage für eine Datenverarbeitung beschritten werden. Zwar sind mit den Konzepten des Broad Consent, Dynamic Consent und Meta Consent bereits Alternativen zur klassischen Einwilligungslösung vorhanden, jedoch können auch diese nicht sämtliche Defizite des Einwilligungsmodells beheben, insbesondere mit Blick auf das Erfordernis einer informierten Einwilligung (Informed Consent).

## Broad, Meta und Dynamic Consent

Schon seit Längerem werden besondere Formen der Einwilligung propagiert, um den Problemen der Unbestimmtheit und der Informationsüberflutung im Einwilligungsprozess zu begegnen. So soll das Konzept des *Broad Consent* in erster Linie dem Umstand Rechnung tragen, dass zu Beginn eines Forschungsprojekts oftmals noch nicht im Detail absehbar ist, zu welchen Zwecken personenbezogene Daten im weiteren Verlauf des Forschungsprojekts verarbeitet werden, sodass die Einwilligung der betroffenen Person nicht bestimmt genug gefasst werden kann. Um dennoch eine wirksame Einwilligung abgeben zu können, können bei einem Broad Consent in Anlehnung an Erwägungsgrund 33 DSGVO Information und Einwilligung auch weiter („breiter“) ausfallen und sich auf „bestimmte Bereiche wissenschaftlicher Forschung“ beziehen. Für die praxisrelevante Forschung an Universitätskliniken in Deutschland hat etwa die Medizin-Informatik-Initiative (MII) eine Handreichung zur Ausgestaltung des Broad Consent erstellt [8], die auch von der Datenschutzkonferenz (DSK; [9]) als datenschutzkonform akzeptiert worden ist [10]. Allerdings zeigt eben diese Handreichung mit ihrer immer noch 7-seitigen Musterinformation [11], dass auch der Broad Consent sehr umfangreiche Informationen für die TeilnehmerInnen bedingt und sich daher letztendlich wieder das Problem einer Informationsüberflutung (Information Overload) stellt [12].

Eine Informationsüberflutung geht regelmäßig auch mit dem Modell des *Meta Consent* einher [13], welches dadurch gekennzeichnet ist, dass Probanden nach einer Beratung entscheiden, für welche Art von Forschungsvorhaben sie in welchem Forschungskontext welche Art von Einwilligung geben möchten und wie und wann sie eine Einwilligung in Zukunft abgeben wollen [14]. Es handelt sich somit um eine Einwilligung bezogen auf zukünftige Einwilligungserklärungen, bei der die zur Auswahl stehenden Einwilligungen optional die klassische spezifische Einwilligung, aber auch den Broad Consent umfassen [14]. Der Meta Consent führt vor allem deshalb zu einem Information Overload, da jeweils beschrieben werden muss, für welche Datenverarbeitungen welche Art von Einwilligung zur Verfügung steht.

Die im Modell des Meta Consent auf einen einzigen Zeitpunkt konzentrierte Informationslast soll im Modell des *Dynamic Consent* vermieden werden. Informationen sollen beim Dynamic Consent über einen längeren Zeitraum hinweg verteilt und es so den TeilnehmerInnen ermöglicht werden, sich je nach individueller Präferenz mehr oder weniger zu engagieren und die eigenen Einwilligungen entsprechend in Echtzeit zu ändern [15]. Wie der Dynamic Consent von Meta oder Broad Consent unterschieden wird, ist bisher wenig transparent, letztendlich dürfte der Dynamic Consent vor allem die Tatsache beschreiben, dass eine technische Infrastruktur verwendet wird, die auf die NutzerInnen zugeschnitten ist und über die sie über einen längeren Zeitraum hinweg neue Einwilligungen abgegeben können [7]. In diesem dynamischen Vorgehen liegt jedoch auch ein entscheidendes Argument gegen den Dynamic Consent, denn bei einer mehrmaligen Interaktion und Information der NutzerInnen ist auch die Gefahr eines Ermüdungseffekts höher – insbesondere wenn die jeweiligen Interaktionen und Informationen zeitlich eng beieinander liegen.

Außerdem können sowohl Broad, Dynamic als auch Meta Consent für sich genommen die grundlegenden Problematiken um die Einwilligung nicht vollständig lösen, denn unabhängig davon, wie oft eine Einwilligung eingeholt wird, bleibt offen, worüber und wie transparent über Datenverarbeitungen informiert werden kann. Insofern lösen auch diese Ansätze nicht die zugrunde liegenden Probleme eines jeden Informed-Consent-Modells – die Überfülle und Überkompliziertheit an Informationen –, sondern konzentrieren diese lediglich auf einen Zeitpunkt (Broad und Meta Consent) bzw. verteilen sie auf mehrere Zeitpunkte (Dynamic Consent).

Bundesgesundheitsbl 2024 · 67:285–291 https://doi.org/10.1007/s00103-024-03835-3


M. Freye · B. Buchner

## Digitale Gesundheitstechnologien – das Recht als Hemmschuh oder Wegbereiter?

**Zusammenfassung**

Der potenzielle Nutzen digitaler Gesundheitstechnologien hängt im Bereich der populationsbezogenen Gesundheitsforschung maßgeblich davon ab, ob und in welchem Umfang sich diese Technologien auf eine Verarbeitung personenbezogener Gesundheitsdaten stützen lassen. Allerdings herrscht erhebliche Unsicherheit bei der Anwendung und Auslegung der einschlägigen rechtlichen Regelungen zur Verarbeitung von Forschungsdaten mittels digitaler Gesundheitstechnologien. Die Praxis der Forschungsdatenverarbeitung ist immer noch maßgeblich vom Primat der Einwilligung als Legitimationsgrundlage für eine Datenverarbeitung geprägt, obwohl das Informationsmodell des deutschen und europäischen Gesetzgebers mit seinen ambitionierten Anforderungen an die freiwillige und informierte Einwilligung realitätsfern ist. Auch die Konzepte des Broad Consent, Dynamic Consent und Meta Consent, die Alternativen zur klassischen Einwilligungslösung darstellen, können nicht sämtliche Defizite des Einwilligungsmodells beheben.

Um die informationelle Selbstbestimmung der betroffenen Personen zu gewährleisten und gleichzeitig die Interessen der Forschung im Public-Health-Bereich im Blick zu behalten, muss der Forschungsdatenschutz weiterentwickelt werden. Lösungen müssen dabei nicht nur am Einwilligungsverhalten selbst ansetzen, sondern auch eine Legitimation der Datenverarbeitung ganz ohne Einwilligung in den Blick nehmen oder auf eine unwiederbringliche Aufhebung des Personenbezugs der Daten abzielen. Dieser Diskussionsartikel beleuchtet die ambivalente Rolle des Rechts im Hinblick auf digitale Gesundheitstechnologien und zeigt, dass der oftmals als Hindernis verstandene Gesundheitsdatenschutz – bei entsprechender Weiterentwicklung – durchaus den Weg für digitale Gesundheitstechnologien bereiten kann.

**Schlüsselwörter**

Broad Consent · Dynamic Consent · DSGVO · European Health Data Space · Opt-out

## Legal regulation of digital public health interventions—hindrance or stimulus?

**Abstract**

The potential benefits of digital health technologies in population-based health research depend mainly on whether and to what extent these technologies can be based on the processing of personal health data. However, there needs to be more certainty in the application and interpretation of the relevant legal regulations on the processing of research data using digital health technologies. Research practice primarily uses consent as a legitimation basis for data processing, although the information model of the German and European legislator, with its ambitious requirements for voluntary and informed consent, is unrealistic and needs to be revised. Even the concepts of broad consent, dynamic consent, and meta consent, which represent alternatives to the classic consent solution, cannot remedy all the deficits of the consent model.

In order to guarantee the informational self-determination of the persons concerned and, at the same time, keep an eye on the interests of research in the public health sector, data protection for research purposes must be further developed. Solutions should not only be tailored to consent behavior but must also consider the legitimization of research data processing without consent or aim to remove the personal reference of the data irretrievably. To date, the law has only fulfilled its task of striking an appropriate balance between the interests of all stakeholders to a limited extent. However, improvement is in sight, especially given current regulatory initiatives and new legal solutions. This discussion article illustrates the ambivalent role of law: on the one hand, health data protection law is often perceived as an obstacle to innovation, but on the other hand, law can pave the way for digital health technologies if further developed.

**Keywords**

Broad consent · Dynamic consent · GDPR · European Health Data Space · Opt-out

## Informiertheit neu gedacht

Um das Problem der Informiertheit der Einwilligung sachgerecht zu adressieren, bedarf es einer grundsätzlich anderen Herangehensweise. Im Fokus sollte nicht die Frage stehen, auf welche andere Art und Weise Informationen präsentiert werden könnten, sondern vielmehr die Frage, welche Informationen überhaupt präsentiert werden sollten – und zwar nicht mit Blick auf ein Mindest-, sondern vielmehr mit Blick auf ein Höchstmaß an Informationen. Ganz anders präsentieren sich die bisherigen Ansätze: Die von der MII vorgeschlagene Musterinformation im Rahmen des Broad Consent betrifft immer noch 16 Aspekte, über die ProbandInnen informiert werden sollen [11]. Die Zusammenstellung ist erkennbar von dem Bestreben getragen, schulmäßig alle Aspekte abzudecken, die irgendwie von datenschutzrechtlicher Relevanz sein könnten. Im gleichen Stil richten auch die vom Europäischen Datenschutzausschuss (EDSA; [16]) und der DSK [17] angesprochenen allgemeinen Mindestinformationen für eine informierte Einwilligung den Fokus darauf, worüber *mindestens* informiert werden soll, und enthalten gerade keine Begrenzung nach oben.[2]

Angesichts der immer weiter voranschreitenden Komplexität der Da-

[2] Beide verweisen darauf, dass zumindest informiert werden muss über die Art der verarbeiteten Daten, die Verantwortlichen der Datenverarbeitung, die Zwecke der Verarbeitung und das Widerrufsrecht sowie – falls anwendbar – über eine Auslandsdatenverarbeitung und eine automatisierte Entscheidung.

tenverarbeitung, gerade bei digitalen Anwendungen, bedarf es aber viel dringender einer Klärung dahingehend, wie ein Informationskatalog aussehen sollte, der nicht unterschritten, vor allem aber auch nicht *überschritten* werden darf, um einer Überforderung und einem Information Overload entgegenzuwirken. Diese Zielrichtung bedingt, dass die Informationspflichten für eine wirksame Einwilligung verdichtet bzw. reduziert werden müssen. Erforderlich ist eine Grenzziehung dahingehend, welche Informationen eine betroffene Person mindestens benötigt – und maximal verarbeiten kann! –, um ihre informationelle Selbstbestimmung tatsächlich souverän und reflektiert wahrnehmen zu können [18]. Entsprechend wird auch in der juristischen Literatur zu Recht eine „verdichtete Informationspräsentation" [19] oder eine „Verschärfung der Wirksamkeitsvoraussetzungen" [20] gefordert. Weniger überzeugen können demgegenüber Ansätze, die die umfangreichen Informationspflichten der Art. 13, 14 DSGVO mit der informierten Einwilligung gleichsetzen und somit davon ausgehen, dass eine wirksame Einwilligung vorliegt, wenn alle Information der Art. 13 und 14 DSGVO bereitgestellt wurden [21–23]. So hat auch der EDSA schon anklingen lassen, dass eine gültige Einwilligung „in informierter Weise" vorliegen kann, selbst wenn nicht alle Elemente der Art. 13 und 14 DSGVO beim Einholen der Einwilligung genannt werden [16, 24, 25].

Welche Informationen für eine informierte Entscheidung elementar sind, sollte künftig vor allem auch unter Einbeziehung der Erkenntnisse anderer Forschungsdisziplinen geklärt werden. Ein solches interdisziplinäres Vorgehen steht in einer Linie mit den Bemühungen der Europäischen Kommission, empirische Entscheidungsforschung in ihre regulatorischen Aktivitäten miteinfließen zu lassen [26, 27]. Insbesondere die Übertragung verhaltenswissenschaftlicher Theorien auf das Einwilligungsverhalten kann Rückschlüsse auf die zu kommunizierenden Informationen vor der Einwilligung liefern und ist gegenüber dem bisherigen Informationsmodell des europäischen Gesetzgebers zumindest im Ansatz empirisch fundiert. Verwiesen sei hier vor allem auf Ansätze, die die Theorie der Schutzmotivation (Protection Motivation Theory – PMT) von Rogers [28] referenzieren und fordern, dass Informationspflichten anhand der PMT entworfen werden müssen [29–33]. Die Forschung hierzu steht jedoch noch ganz am Anfang und es gibt erst wenige Arbeiten, die *konkrete* Informationspflichten in diesem Sinne konzipieren, beispielsweise zur Cookie-Einwilligung [34] oder zur Einwilligung bei Gesundheits-Apps (siehe Dissertationsschrift von Freye M, Publikation vsl. 2024).

## Einwilligungsunabhängige Lösungsansätze

Selbst in Anbetracht der oben dargestellten Ansätze, der Einwilligung als Erlaubnistatbestand zu mehr Legitimationskraft zu verhelfen, bleibt es fraglich, ob die Einwilligung in der Realität je die rechtlichen Idealvoraussetzungen erfüllen kann – auch mit Blick darauf, dass der hier diskutierte Aspekt der Informiertheit nur *einer* der Problempunkte ist, die die Einwilligung als Erlaubnistatbestand kennzeichnen. Gleichermaßen problematisch ist der Aspekt der Freiwilligkeit einer Einwilligung: Was ist etwa von der „Freiwilligkeit" einer Einwilligung in die Nutzung von Apps zur Nachverfolgung von Kontakten zu Infizierten (Contact-tracing-Apps) zu halten, wenn ohne diese die Teilnahme am sozialen Leben ganz erheblich eingeschränkt wird? Wie „freiwillig" ist eine Einwilligung bei medizinischen Forschungsprojekten, wenn die betroffene Person als PatientIn um eine Teilnahme ersucht wird? Wenig kompatibel mit den Bedürfnissen der Forschung ist auch die im Datenschutzrecht angelegte freie Widerrufbarkeit der Einwilligung. Ein solcher Widerruf der Einwilligung erfordert nicht nur aufwändige Mechanismen, um den Widerruf im konkreten Fall im Datenbestand umsetzen zu können, sondern läuft darüber hinaus auch dem Forschungsinteresse an einer stabilen und langfristigen Datengrundlage, die insbesondere für epidemiologische Analysen entscheidend ist, zuwider. Letzteres Problem stellt sich ebenso, wenn und soweit man ein mögliches „Verfallsdatum" der Einwilligung in Betracht zieht [35]. Zu guter Letzt streiten auch die Aspekte der Datenqualität und einer möglichst vollständigen und damit aussagekräftigen Datenbasis (Repräsentativität) gegen den Weg über die Einwilligung [7].

Vor diesem Hintergrund sprechen gute Gründe für Lösungsansätze, die auf eine Legitimation der Forschungsdatenverarbeitung ganz ohne Einwilligung setzen. Teils finden sich solcherlei Modelle schon im geltenden Recht, hierzulande etwa in der Vorschrift des § 27 BDSG, die die entsprechende Öffnungsklausel des Art. 9 Abs. 2 lit. j DSGVO ausformt. Zulässig ist danach eine Verarbeitung besonderer Kategorien personenbezogener Daten u. a. zu wissenschaftlichen Forschungszwecken auch ohne Einwilligung, wenn die Verarbeitung für diese Zwecke erforderlich ist und die Interessen der verantwortlichen Stelle an der Verarbeitung die Interessen der betroffenen Person an der Nichtverarbeitung der Daten erheblich überwiegen.

Auch andere aktuelle Gesetzgebungsinitiativen setzen auf einwilligungsunabhängige Lösungskonzepte, auf deutscher ebenso wie auf europäischer Ebene. So soll mit dem kürzlich erschienenen Referentenentwurf zu einem deutschen Gesundheitsdatennutzungsgesetz (GDNG-E) insbesondere die Freigabe von Daten der elektronischen Patientenakte (ePA) an das Forschungsdatenzentrum ohne Einwilligung auskommen und lediglich eine Widerspruchsoption (Opt-out) enthalten (GDNG-E, S. 18, 48). Auf europäischer Ebene beschreibt außerdem die in dem Entwurf für eine Verordnung über den europäischen Raum für Gesundheitsdaten (EHDS-VO-E) vorgesehene Datengenehmigung eine einwilligungsfreie Lösung, die von einer Zugangsstelle für die Sekundärnutzung von Gesundheitsdaten ausgestellt wird – und zwar ohne Einwilligung der betroffenen Person, Art. 46 Abs. 1 EHDS-VO-E.

Die Legitimationskraft all dieser einwilligungsunabhängigen Lösungen hängt ganz wesentlich davon ab, dass der Wesensgehalt des Rechts auf Datenschutz gewahrt bleibt und umfangreiche technische und organisatorische Maßnahmen zur Wahrung der Grundrechte

und Interessen der betroffenen Person vorgesehen werden. Hierzu muss insbesondere eine Widerspruchsoption zählen, die der betroffenen Person ein Opt-out jederzeit und ohne Angaben von Gründen so leicht wie möglich macht [36, 37]. Schon die DSK stellte in der Petersberger Erklärung die Widerspruchsmöglichkeit der betroffenen Person als ein wesentliches Element einer einwilligungsunabhängigen Rechtfertigung heraus [38]. Aus diesem Grund ist es ebenso konsequent wie sachgerecht, dass die oben dargestellten einwilligungsfreien Lösungen, die aktuell für die ePA und im GDNG vorgesehen sind, mit einem entsprechenden Widerrufsrecht verknüpft werden.

Zu weit ging daher auch der ursprüngliche Entwurf der Kommission für die EHDS-VO aus dem Jahr 2022, der keine ausdrückliche Widerspruchsoption enthielt, sodass bereits ein totaler Bedeutungsverlust nationaler Opt-out-Regelungen prognostiziert wurde [39, 40] und damit der Einzelne jeglicher Form einer digitalen Souveränität beraubt worden wäre. Für eine Ergänzung der EHDS-VO um eine Opt-out-Lösung, wie sie dann auch in den zweiten Kompromisstext des Rats aufgenommen worden ist, sprechen nicht zuletzt ganz praktische Erwägungen: Erfahrungsgemäß wird ein Widerspruch ohnehin nur ganz selten ausgeübt [41][3] und sollte ein Forschungsvorhaben im Einzelfall aufgrund massenhafter Ausübung des Widerrufs tatsächlich zu scheitern drohen, kommt ausnahmsweise auch noch ein Ausschluss des Widerrufsrechts zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe nach Art. 21 Abs. 6 Hs. 2. DSGVO in Betracht. Angesichts des mit einem Widerrufsrecht einhergehenden Souveränitätsgewinns für die betroffenen Personen und der Praxistauglichkeit entspricht das Widerrufsrecht genau dem erklärten Ziel des EHDS, einen gemeinsamen Raum zu schaffen, in dem einerseits natürliche Personen ihre elektronischen Gesundheitsdaten leicht und selbstbestimmt kontrollieren können, es andererseits aber auch AkteurInnen aus Forschung und Innovation sowie politischen EntscheidungsträgerInnen ermöglicht wird, diese elektronischen Gesundheitsdaten auf vertrauenswürdige und sichere Weise unter Wahrung der Privatsphäre zu nutzen (EHDS-VO-E).

## Aufhebung des Personenbezugs als Ausweg?

Unabhängig von den zuvor dargestellten Initiativen und Lösungsansätzen kann schließlich auch über den Weg der Datenanonymisierung eine leicht(er) zugängliche Datengrundlage für die Forschung eröffnet werden [42], da die DSGVO nur für die Verarbeitung von personenbezogenen Daten gilt, nicht jedoch für anonymisierte Daten. Gerade in der Public-Health-Forschung ist allerdings der Weg über die Anonymisierung oftmals schon deshalb verschlossen, weil es bei einer unwiederbringlichen Aufhebung des Personenbezugs auch nicht mehr möglich wäre, die einzelnen ProbandInnen für wiederholte Kontaktaufnahmen, Rückfragen oder auch für Informationen über eventuell festgestellte Erkrankungen und Diagnosen kontaktieren zu können [10]. Eine wiederholte Kontaktaufnahme ist gerade bei Langzeitstudien unerlässlich, die auf einem Follow-up-Konzept beruhen, wie etwa die NAKO-Gesundheitsstudie, das Sozio-oekonomische Panel (SOEP) oder die britische Kohortenstudie BCS70. Auch bei einer mehrstufigen Delphi-Befragung, die über eine digitale Plattform geschaltet wird, ist eine Pseudonymisierung unabdingbar, um untersuchen zu können, ob die Befragten ihre Meinung während der verschiedenen Befragungsrunden geändert haben. Sollen Daten aus am Körper getragenen Computern (Wearables) mit weiteren Daten verknüpft werden, erfordert diese Datenverknüpfung ebenfalls eine Pseudonymisierung, die sicherstellt, dass die zusammengeführten Daten dieselbe Person betreffen.

Werden Daten zum Zweck der Rückverfolgbarkeit oder Verknüpfung nur pseudonymisiert, nicht aber anonymisiert, sind diese nach herrschender Meinung als personenbezogen einzuordnen und fallen damit in den Anwendungsbereich des Datenschutzrechts. Möglicherweise löst sich die starre Zweiteilung in anonymisiert und pseudonymisiert zukünftig aber auf, wenn anknüpfend an eine Entscheidung des Gerichts der Europäischen Union (EuG) vom April 2023 die Aufhebung eines Personenbezugs von Daten auch für den Fall der Pseudonymisierung zumindest nicht mehr pauschal auszuschließen ist [43]. Das EuG stellte in dieser Entscheidung fest, dass auch eine Pseudonymisierung unter bestimmten Umständen den Personenbezug von Daten entfallen lassen kann, wenn – wie im entschiedenen Fall – pseudonymisierte Daten an eine dritte Stelle weitergegeben werden, die selbst nicht über die Mittel verfügt, um den Personenbezug herzustellen [43]. Diese „anonymisierende Pseudonymisierung" [44, 45] ist letztendlich eine konsequente Umsetzung der sog. relativen Theorie im Datenschutzrecht, die der Europäische Gerichtshof (EuGH) schon seiner Entscheidung in der Rechtssache Breyer zugrunde gelegt hat [46] und nach der zur Beurteilung eines Personenbezugs eine Risikoprognose erforderlich ist, die auf die Wahrscheinlichkeit von Reidentifizierungsrisiken *der jeweiligen datenverarbeitenden Stelle* abstellt [47].

Setzt sich dieses Verständnis, wie aktuell vom EuG forciert, in der datenschutzrechtlichen Diskussion durch, eröffnen sich vor allem mit dem Modell der Datentreuhand in ganz weitem Umfang Möglichkeiten einer Datenverarbeitung zu Forschungszwecken. Pseudonymisierte Daten wären dann nur noch für diejenige datenverarbeitende Stelle als personenbezogene Daten einzuordnen, die die Zuordnungsregel für ein Pseudonym vergibt und dieses Pseudonym verwaltet – in der Treuhandkonstellation also die Treuhandstelle selbst. Nicht aber wären diese Daten auch für sonstige datenverarbeitende Stellen, die diese pseudonymisierten Daten (für Forschungszwecke) nutzen, als personenbezogene Daten einzuordnen. Dies gilt jedenfalls dann, wenn es sich bei der Treuhandstelle um eine Stelle handelt, die

[3] Beispielhaft verwiesen sei hier nur auf die Widerspruchsquote von gerade einmal 2 % aller KrebspatientInnen, die laut Bayerischem Landesbeauftragten für den Datenschutz (BayLfD) Prof. Dr. Thomas Petri in Bayern einer Übertragung ihrer Gesundheitsdaten ins Krebsregister widersprechen [41].

mit besonderen Vertraulichkeitspflichten und -rechten ausgestattet ist und deshalb mit hinreichender Sicherheit ausgeschlossen werden kann, dass diese Stelle den Personenbezug der pseudonymisierten Daten gegenüber anderen Stellen wieder offenlegt. Entscheidend ist, dass es für die forschenden Stellen keinen rechtlich möglichen Weg geben darf, die Zuordnungsregel zu erfahren, und auch kein anderer praktisch gangbarer Weg besteht, um mit einem verhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften an die Zuordnungsregel zu gelangen [43, 44, 48].

## Fazit

Der Befund, dass das Datenschutzrecht für die populationsbezogene Gesundheitsforschung an und mit digitalen Gesundheitstechnologien bislang eher Hemmschuh als Wegbereiter ist, hat durchaus seine Berechtigung. Umso wichtiger sind daher neue Impulse aus Wissenschaft, Gesetzgebung und Rechtsprechung für ein forschungsfreundlicheres Datenschutzrecht.

Im Rahmen des bisherigen Einwilligungsmodells zielen neue Lösungsansätze vor allem darauf ab, jenseits von Broad, Dynamic und Meta Consent Informationspflichten neu zu konzipieren, um sicherzustellen, dass die Betroffenen weder mit Informationen überflutet noch von zu komplizierten Informationen überfordert werden.

Aktuelle Gesetzesvorhaben schlagen hingegen einen Weg ein, der von vornherein nicht über die Einwilligung führt, sondern darauf abzielt, einwilligungsunabhängige Legitimationstatbestände auszugestalten. Die zentrale Rolle der Einwilligung soll abgelöst werden durch andere Formen digitaler Souveränität, wie insbesondere die Möglichkeit des Opt-out. Mit dem GDNG-E und dem EHDS-VO-E stehen neue Lösungsmodelle vor der Tür, die das Interesse an einer repräsentativen Datenbasis mit dem Schutz informationeller Selbstbestimmung jenseits des Einwilligungsprimats in einen Ausgleich bringen.

Schließlich kann auch der Personenbezug von Daten neu gedacht werden, wenn die bis dato sehr schematisch gehaltene Zweiteilung von pseudonymisierten und anonymisierten Daten aufgebrochen wird und damit vor allem auch Lösungen über eine Datentreuhand zur Umsetzung in der Praxis verholfen werden kann.


## Korrespondenzadresse

**Merle Freye**
Institut für Informations-, Gesundheits- und Medizinrecht, Universität Bremen
Universitätsallee GW1, 28359 Bremen, Deutschland
mfreye@uni-bremen.de


**Funding.** Open Access funding enabled and organized by Projekt DEAL.

## Einhaltung ethischer Richtlinien

**Interessenkonflikt.** M. Freye und B. Buchner geben an, dass kein Interessenkonflikt besteht.

Für diesen Beitrag wurden von den Autor/-innen keine Studien an Menschen oder Tieren durchgeführt. Für die aufgeführten Studien gelten die jeweils dort angegebenen ethischen Richtlinien.



## Literatur


1. Albrecht U-V (2016) Chancen und Risiken von Gesundheits-Apps (CHARISMHA). https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/Abschlussbericht_CHARISMHA.pdf. Zugegriffen: 15. Aug. 2023
2. OECD (2017) Ministerial statement. https://www.oecd.org/health/ministerial-statement-2017.pdf. Zugegriffen: 15. Aug. 2023
3. Cepic M (2021) Broad Consent: Die erweiterte Einwilligung in der Forschung. ZD-Aktuell 10:5214
4. Roßnagel A (2019) Datenschutz in der Forschung. ZD 9:157–164
5. Roßnagel A (2023) Datenschutz und Forschung Beziehungsstatus: kompliziert. https://www.medical-tribune.de/meinung-und-dialog/artikel/beziehungsstatus-kompliziert. Zugegriffen: 15. Aug. 2023
6. Deutsches Ärzteblatt (2022) Datenschutz darf kein Hemmschuh für Forschung sein. https://www.aerzteblatt.de/nachrichten/136389/Datenschutz-darf-kein-Hemmschuh-fuer-Forschung-sein. Zugegriffen: 15. Aug. 2023
7. Hummel P, Braun M, Augsberg S, von Ulmenstein U, Dabrock P (2021) Dynamic Consent als Umsetzungsmechanismus von Datensouveränität. In: Hummel P, Braun M, Augsberg S, von Ulmenstein U, Dabrock P (Hrsg) Datensouveränität. Governance-Ansätze für den Gesundheitsbereich. Springer VS, Wiesbaden, S 13–20
8. AG Consent der Medizininformatik-Initiative (2023) Handreichung zur Anwendung der national harmonisierten Patienteninformations- und Einwilligungsdokumente zur Sekundärnutzung von Patientendaten AG Consent der Medizininformatik-Initiative (MII). Version 1.3. https://www.medizininformatik-initiative.de/sites/default/files/2023-05/MII_AG-Consent_Handreichung_v1.3.pdf. Zugegriffen: 15. Aug. 2023
9. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2020) Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu den Einwilligungsdokumenten der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung. https://www.datenschutzkonferenz-online.de/media/dskb/20200427_Beschluss_MII.pdf. Zugegriffen: 15. Aug. 2023
10. Weichert T (2022) Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung – Vorgaben der EU-Datenschutz-Grundverordnung und national geltender Gesetze. Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin
11. AG Consent der Medizininformatik-Initiative (2020) Mustertext Patienteneinwilligung. Version 1.6 d. https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf. Zugegriffen: 15. Aug. 2023
12. Fröhlich W, Döhmann I (2022) Die breite Einwilligung (Broad Consent) in die Datenverarbeitung zu medizinischen Forschungszwecken – der aktuelle Irrweg der MII. GesR 6:346–353. https://doi.org/10.9785/gesr-2022-210605
13. Datenethikkommission (2019) Gutachten der Datenethikkommission. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6. Zugegriffen: 15. Aug. 2023
14. Ploug T, Holm S (2016) Meta consent—A flexible solution to the problem of secondary use of health data. Bioethics 30:721–732. https://doi.org/10.1111/bioe.12286
15. Kaye J, Whitley E, Lund D, Morrison M, Teare H, Melham K (2015) Dynamic consent: a patient interface for twenty-first century research networks. Eur J Hum Genet 23:141–146. https://doi.org/10.1038/ejhg.2014.71
16. Europäischer Datenschutzausschuss (2020) zur Einwilligung gemäß Verordnung 2016/679. Version 1.1. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf. Zugegriffen: 15. Aug. 2023

17. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2019) Kurzpapier Nr. 20. https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf. Zugegriffen: 15. Aug. 2023
18. Lurger B (2018) Die hohe Informationslast beim Abschluss von Verträgen. Wie entscheiden Verbraucherinnen und Verbraucher wirklich und wie könnte sie das Recht dabei besser unterstützen. In: Nessel S, Tröger N, Fridrich C, Hübner R (Hrsg) Multiperspektivische Verbraucherforschung. Ansätze und Perspektiven. Springer VS, Wiesbaden, S 113–138
19. Geminn CL, Francis L, Herder K-R (2021) Die Informationspräsentation im Datenschutzrecht – Auf der Suche nach Lösungen. ZD Aktuell 2021:5335
20. Radlanski P (2016) Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Dissertation, Universität Regensburg
21. Schmidt-Wudy F (2023) Art. 13 DSGVO Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person. In: Wolff HA, Brink S, von Ungern-Sternberg A (Hrsg) BeckOK Datenschutzrecht DS-GVO, BDSG, Grundlagen, Bereichsspezifischer Datenschutz. 44. Edition C. H. Beck. C. H. Beck, München
22. Dix A (2019) Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person. In: Simitis S, Hornung G, Döhmann (Hrsg) Datenschutzrecht. Nomos, Baden-Baden, S 630–639
23. Mester BA (2022) Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person. In: Taeger J, Gabel D (Hrsg) DSGVO BDSG, 4. Aufl. Recht und Wirtschaft, Frankfurt a. M., S 468–487
24. Art.-29-Datenschutzgruppe (2018) Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679. WP 259 rev.01. https://www.datenschutzstelle.li/application/files/3615/3674/7263/wp259rev01_de.pdf. Zugegriffen: 15. Aug. 2023
25. Europäischer Datenschutzausschuss (2018) Endorsement 1/2018. https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf. Zugegriffen: 15. Aug. 2023
26. Sousa Lourenço J, Ciriolo E, Rafael Almeida R, Troussard X (2016) Behavioural insights applied to policy: European report https://doi.org/10.2760/903938
27. European Commission, Joint Research Centre (2022) Ex post evaluation of the activities of the Joint Research Centre under Horizon 2020 and Euratom 2014–2020: final report of the ex post evaluation panel https://doi.org/10.2760/257315
28. Rogers RW (1983) Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo JT, Petty RT (Hrsg) Social psychophysiology: a sourcebook. Guilford, New York, S 153–177
29. Boerman SC, Kruikemeier S, Zuiderveen Borgesius FJ (2018) Exploring motivations for online privacy protection behavior: insights from panel data. Communic Res 7:953–977. https://doi.org/10.1177/0093650218800915
30. Helberger N, Lynskey O, Micklitz H-W, Rott P, Sax M, Strycharz J (2021) EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf. Zugegriffen: 15. Aug. 2023
31. Meier Y, Schäwel J, Kyewski E, Krämer NC (2020) Applying protection motivation theory to predict Facebook users' withdrawal and disclosure intentions. In: Gruzd A, Mai P, Recuero R, Hernandez-Garcia A, Lee CS, Cook J et al (Hrsg) SMsociety'20: international conference on social media and society. Association for Computing Machinery, Toronto, S 21–29 https://doi.org/10.1145/3400806.3400810
32. Strycharz J, van Noort G, Smit E, Helberger N (2019) Protective behavior against personalized ads: Motivation to turn personalization off. Cyberpsychology 13(2):1. https://doi.org/10.5817/CP2019-2-1
33. Wottrich V, van Reijmersdal EA, Smit EG (2019) App users unwittingly in the spotlight: a model of privacy protection in mobile Apps. J Consum Aff 3:1056–1083. https://doi.org/10.1111/joca.12218
34. Chennamaneni A, Gupta B (2022) The privacy protection behaviours of the mobile app users: exploring the role of neuroticism and protection motivation theory. Behav Inf Technol. https://doi.org/10.1080/0144929X.2022.2106307
35. Rolfs J (2020) Die zeitliche Wirkungsdauer der datenschutzrechtlichen Einwilligung – das „absolute" und „relative" Verfallsdatum. In: Specht-Riemenschneider L, Buchner B, Heinze C, Thomsen O (Hrsg) IT-Recht in Wissenschaft und Praxis. Festschrift für Jürgen Taeger. Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft„ Frankfurt a. M., S 373–391
36. Buchner B (2023) Digitales Gesundheitswesen x.0. Zgi Editor 2:53–54
37. Petri T (2022) Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten. Zum Vorschlag der EU-Kommission für einen Europäischen Gesundheitsdatenraum. DuD 46:413–418. https://doi.org/10.1007/s11623-022-1631-6
38. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2022) Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiHw8jgq-GAAxXEVvEDHUS2DnMQFnoECBgQAQ&url=https%3A%2F%2Fwww.datenschutzkonferenz-online.de%2Fmedia%2Fen%2F20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf&usg=AOvVaw0ywVZXJTkRt-3sEf0Nr8kW&opi=89978449. Zugegriffen: 15. Aug. 2023
39. Gassner U (2023) Essentialia eines Gesundheitsdatennutzungsgesetzes. ZRP 56:34–37
40. Roos P, Maddaloni JM (2023) Regulierter Datenaustausch zur Gesundheitsforschung. Die legislativen Vorhaben für einen Europäischen Gesundheitsdatenraum und ein Gesundheitsdatennutzungsgesetz. RDi 3:225–232
41. Hilbricht B (2023) Gesundheitsdaten EU-weit teilen. https://www.behoerden-spiegel.de/2023/02/13/gesundheitsdaten-eu-weit-teilen/. Zugegriffen: 15. Aug. 2023
42. Hofmann S (2022) Forschungsklausel statt Broad Consent. Sekundärnutzung von Patientendaten ohne Einwilligung, dafür mit Opt-out. DuD 46:756–761. https://doi.org/10.1007/s11623-022-1691-7
43. EuG Urteil v. 26. April 2023 – T-557/20, ECLI:EU:T:2023:219.
44. Roßnagel A (2018) Pseudonymisierung personenbezogener Daten. Ein zentrales Instrument im Datenschutz nach der DS-GVO. ZD 9:243–247
45. Baumgartner U (2023) Anmerkung zu EuG Urteil v. 26. April 2023 – T-557/20. ZD 13:402–404
46. EuGH Urteil v. 19. Oktober 2016 – C-582/14, ECLI:EU:C:2016:779 – Breyer.
47. Klar M, Kühling J (2020) Art. 4 Nr. 1 DS-GVO Begriffsbestimmungen personenbezogene Daten. In: Kühling J, Buchner B (Hrsg) DS-GVO BDSG, 3. Aufl. C.H. Beck, München, S 147–159
48. Buchner B (2020) Grundsätze des Datenschutzrechts. In: Tinnefeld M-T, Buchner B, Petri T, Hof H-J (Hrsg) Einführung in das Datenschutzrecht, 7. Aufl. De Gruyter Oldenbourg, Berlin, S 220–327