BDI

Gesundheit digital
BDI initiativ

POSITION | GESUNDHEITS- UND WIRTSCHAFTSPOLITIK | IGW

Datenschutzhürden in der industriellen Gesundheitswirtschaft

Handlungsempfehlungen zur rechtssicheren Nutzung von Gesundheitsdaten

2. Juli 2025

Executive Summary

Die industrielle Gesundheitswirtschaft (iGW) ist ein zentraler Innovationstreiber und systemrelevant für eine zukunftsfähige Gesundheitsversorgung. Ihre Leistungsfähigkeit basiert maßgeblich auf der intelligenten Nutzung medizinischer Daten – etwa für die Entwicklung neuer Therapien, digitaler Medizintechnologien sowie innovativer Anwendungen in Versorgung und Produktion. Gleichzeitig ist sie mit einer Million Beschäftigten, hoher Exportstärke und einer Bruttowertschöpfung von 103 Milliarden Euro ein bedeutender Wirtschafts- und Standortfaktor. Um dieses Potenzial zu heben, braucht es einen innovationsfreundlichen und rechtssicheren Datenschutzrahmen.

Die bisweilen uneinheitliche Auslegung datenschutzrechtlicher Vorgaben erschwert die Durchführung von Forschungsprojekten, bremst medizinische Innovationen aus und gefährdet Deutschlands Anschlussfähigkeit im europäischen Gesundheitsdatenraum; verstärkt wird dies durch eine Heterogenität der Rechtslage: So enthalten etwa Landeskrankenhausgesetze unterschiedliche und teils unklare, rechtliche Vorgaben, die Auswirkungen auf die Datenweitergabe zu Forschungszwecken oder die Einbindung externer Auftragsverarbeiter haben.

Während andere europäische Länder unter derselben europäischen Datenschutzgrundverordnung (DSGVO) pragmatischere Wege finden, Gesundheitsdaten sowohl für Forschungszwecke als auch für innovative Versorgungslösungen und Geschäftsmodelle nutzbar zu machen, erschwert in Deutschland ein komplexes, uneinheitliches Regelwerk die Forschungs- und Entwicklungsarbeit erheblich. Dies beeinträchtigt nicht nur die Innovationskraft der iGW, sondern auch ihre Resilienz in einem zunehmend dynamischen globalen Umfeld. Ein ineffizienter und rechtsunsicherer Zugang zu Gesundheitsdaten schwächt die internationale Wettbewerbsfähigkeit und zwingt Forschungseinrichtungen und Unternehmen zunehmend dazu, Studieninfrastrukturen und Technologien im Ausland zu nutzen, obwohl ausländische Versorgungsdaten nur begrenzt auf den deutschen Kontext übertragbar sind.

Der Koalitionsvertrag 2025 greift diese Herausforderungen auf und kündigt einheitliche Auslegungen und Vereinfachungen beim Datenschutz an, u. a. durch eine Reform der Datenschutzaufsicht, der Bündelung von Kompetenzen bei der Bundesdatenschutzbeauftragten und einer stärkeren Betrachtung der Datennutzung bei gleichzeitiger Maxime des Datenschutzes. Aus Sicht der iGW sind jedoch weitergehende Maßnahmen auf sämtlichen Zuständigkeitsebenen erforderlich, um die notwendige Rechtssicherheit und Interoperabilität entlang der gesamten Wertschöpfungskette zu schaffen.

Maria Kusmina | Industrielle Gesundheitswirtschaft | T: +49 30 2028-1505 | m.kusmina@bdi.eu | www.bdi.eu

Vor diesem Hintergrund fasst die vorliegende Position die zentralen Datenschutzhürden für die gesamte iGW zusammen und formuliert konkrete Handlungsempfehlungen zur rechtssicheren Nutzung von Gesundheitsdaten – entlang der folgenden Struktur:

1. **Zentrale Datenschutzaufsicht für Gesundheitsdaten schaffen**: Die Auslegung datenschutzrechtlicher Vorgaben im Gesundheitswesen ist derzeit stark fragmentiert. Eine zentrale Aufsicht für Gesundheitsdaten würde bundesweit einheitliche Maßstäbe schaffen, Koordinationsaufwände senken und die Rechtssicherheit bei der Nutzung medizinischer Daten für Forschung und Versorgung erhöhen.

   Handlungsebene: Bundesgesetzgeber, Datenschutzaufsichtsbehörden

2. **Forschung und digitale Innovation datenschutzkonform ermöglichen**: Einheitliche und forschungsfreundliche rechtliche Rahmenbedingungen sind Voraussetzung für datengetriebene Forschung. Die Beseitigung des gesetzlichen Flickenteppichs gehört dabei ebenso dazu, wie eine ermöglichende Ausgestaltung und Anwendung der Forschungsklauseln nach Art. 89 DSGVO und § 27 BDSG. Dabei ergibt sich die Notwendigkeit einer praxistauglichen Definition von Forschung, die auch von privatwirtschaftlichen Unternehmen ermöglicht wird (z. B. Pharma-Unternehmen, E-Health-Datenunternehmen).

   Handlungsebene: Bundes- und Landesgesetzgeber, Datenschutzaufsichtsbehörden.

3. **Rechtssicherheit bei Anonymisierung und Pseudonymisierung schaffen**: Bei der Nutzung großer Gesundheitsdatensätze zu Forschungszwecken besteht häufig Rechtsunsicherheit darüber, wann Daten ausreichend anonymisiert bzw. pseudonymisiert sind; das gilt insbesondere bei Bilddaten und Bioproben. Es braucht praxistaugliche, bundeseinheitlich anerkannte Definitionen und Standards, die sich am Grundsatz der Anonymisierung ausrichten und die datenschutzkonforme Nutzung langfristig ermöglichen.

   Handlungsebene: Bundesgesetzgeber, Datenschutzaufsichtsbehörden, EU-Ebene.

4. **Datenschutzgerechte Integration digitaler Versorgungstechnologien sicherstellen**: Digitale Anwendungen in der Versorgung erfordern eine zentrale Verarbeitung medizinischer Daten über Einrichtungs- und Landesgrenzen hinweg. Die datenschutzrechtlichen Voraussetzungen dafür sollten bundesweit vereinheitlicht und technologieoffen geregelt werden.

   Handlungsebene: Bundes- und Landesgesetzgeber, Datenschutzaufsichtsbehörden.

5. **Internationale Datennutzung und europäische Anschlussfähigkeit sichern:** Datenschutz darf kein Standortnachteil sein. Für grenzüberschreitende Kooperationen, Zulassungsverfahren und Cloud-basierte Lösungen braucht es praktikable, rechtssichere Regelungen für den internationalen Datentransfer und die Orientierung an internationalen Standards. Die Spielräume des nationalen Gesetzgebers im Rahmen der Implementierung des European Health Data Space (EHDS) muss forschungsfreundlich genutzt werden, z. B. durch die Anwendung des Opt-out-Prinzips bei der Forschung mit genetischen Daten.

   Handlungsebene: Bundesgesetzgeber, EU-Ebene, Datenschutzaufsichtsbehörde.

Zentrale Datenschutzaufsicht für Gesundheitsdaten schaffen

Die datenschutzrechtliche Steuerung in Deutschland ist durch eine föderale Zuständigkeitsverteilung und eine uneinheitliche Auslegung geprägt. Insgesamt 18 Datenschutzaufsichtsbehörden – eine Bundesbeauftragte sowie 17 Landesdatenschutzbehörden – vertreten teils unterschiedliche Auffassungen, insbesondere beim Teilen von Gesundheitsdaten mit Forschungspartnern und der Übermittlung an externe Auftragsverarbeiter. Diese Uneinheitlichkeit wird dadurch verstärkt, dass rechtliche Voraussetzungen für den Datenaustausch und die Bewertung konkreter Anwendungsfälle je nach Bundesland unterschiedlich interpretiert werden.

Obwohl das Gesundheitsdatennutzungsgesetz (GDNG) eine einheitliche Nutzung von Gesundheitsdaten für Forschungszwecke anstrebt und die Einrichtung einer federführenden Datenschutzaufsicht vorsieht, bleiben die vorgesehenen Koordinierungsmechanismen bislang weitgehend wirkungslos – nicht zuletzt, weil der zentralen Stelle die notwendigen Durchgriffsrechte gegenüber den Landesbehörden fehlen, etwa bei begrenzten Datensätzen wie in den Krebsregistern oder mangels klar definierter Zuständigkeiten und Anwendungsbereiche. Der im Koalitionsvertrag der Bundesregierung verankerte Ansatz, die Datenschutzaufsicht zu reformieren und im Interesse der von Forschung und Wirtschaft zu zentralisieren, ist hierbei ein guter Lösungsansatz.

Föderale Datenschutzvorgaben harmonisieren und Rechtsklarheit schaffen

Die derzeitige Fragmentierung der Rechtslage erzeugt erhebliche Unsicherheit für datengetriebene Projekte in der iGW: Neben der DSGVO und dem Bundesdatenschutzgesetz bestehen 16 Landesdatenschutzgesetze, 16 Landeskrankenhausgesetze mit spezifischen Datenschutzbestimmungen sowie separate Datenschutzgesetze der katholischen und evangelischen Kirche. Ergänzt durch diverse Spezialgesetze ergibt sich ein rechtlicher Flickenteppich, der eine verlässliche rechtliche Einordnung erschwert und die Planung sowie Durchführung von Innovationsvorhaben mit erheblichem Mehraufwand belastet – zum strukturellen Nachteil Deutschlands als Standort für Gesundheitsinnovationen.

Zudem führt die föderale Zersplitterung zu einem überdurchschnittlich hohen administrativen Aufwand: Bundesweit tätige Unternehmen und Kliniken müssen in jedem Bundesland eigene Fachkompetenz für die jeweiligen landesspezifischen Vorgaben vorhalten. Die daraus resultierenden komplexen und zeitintensiven Genehmigungsprozesse binden erhebliche Ressourcen, verursachen hohe Kosten und verzögern dringend benötigte Innovationen. Die Sorge vor Datenschutzverstößen und Bußgeldern führt bei Kliniken, Ethikkommissionen und Unternehmen zu einer restriktiven und oft übervorsichtigen Auslegung. Das bremst nicht nur Forschungsprojekte aus, sondern erschwert auch den rechtskonformen Einsatz digitaler Technologien im Versorgungsalltag. In der Konsequenz werden viele datenbasierte Forschungsvorhaben zu anderen Standorten verlagert.

- ***Bundesweite Koordinierung durch zentrale Datenschutzaufsicht stärken:*** *Zur koordinierenden und rechtssicheren Bewertung datenschutzrechtlicher Fragen in der Gesundheitsforschung sollte die im GDNG vorgesehene federführende Datenschutzaufsicht konsequent umgesetzt, mit klar definierten Zuständigkeiten ausgestattet und operativ gestärkt werden. Nur so kann sie länderübergreifende Vorhaben wirksam begleiten und für eine einheitliche Anwendung der datenschutzrechtlichen Vorgaben sorgen. Das würde auch die gegenseitige Anerkennung von datenschutzrechtlichen Bewertungen zwischen den Bundesländern erleichtern.*
- ***Verlagerung der Aufsichtskompetenzen auf Bundesebene prüfen:*** *Im Sinne einer einheitlichen Aufsichtspraxis im Gesundheitsdatenschutz sollte mittelfristig eine Verlagerung der zentralen Aufsichtskompetenzen auf Bundesebene angestrebt werden. Hierdurch ließen sich uneinheitliche länderspezifische Interpretationen dauerhaft überwinden und eine klare datenschutzrechtliche Grundlage für Forschung und Versorgung schaffen.*

- ***Heterogenität datenschutzrechtlicher Anforderungen abbauen:*** *Unterschiedliche Vorschriften auf Bundes-, Landes- und kirchlicher Ebene erschweren die rechtssichere Nutzung von Gesundheitsdaten erheblich. Notwendig ist ein einheitlicher, rechtssicherer Datenschutzrahmen für Forschung und Versorgung, der widersprüchliche Vorgaben harmonisiert und zentrale Grundsatzfragen, etwa zur Abgrenzung von Verantwortlichkeit und Auftragsverarbeitung, einheitlich klärt.*
- ***Landesrechtliche Sonderregelungen im Datenschutz abbauen:*** *Die DSGVO bietet bereits einen europaweit einheitlichen Rahmen für die Auftragsverarbeitung personenbezogener Daten. Die zusätzlichen landesspezifischen Datenschutzvorgaben in den Krankenhausgesetzen führen zu einer zersplitterten Rechtslage mit erheblichem Zusatzaufwand für alle Beteiligten. Es sollte klargestellt werden, dass die Regelungen der DSGVO für die Datenverarbeitung im Krankenhausbereich ausreichen und keiner ergänzenden landesrechtlichen Regelung bedürfen. Die Streichung landes- und kirchenrechtlicher Regelungen sollte angestrebt werden.*

Forschung und digitale Innovation datenschutzkonform ermöglichen

Mit einer Forschungs- und Entwicklungsintensität von rund 15 Prozent an der Bruttowertschöpfung zählt die iGW zu den forschungsintensivsten Branchen in Deutschland. Ihre Innovationskraft hängt maßgeblich von der Nutzung medizinischer Versorgungsdaten ab. Ein effizienter Zugang zu diesen Daten und ihre sinnvolle Verknüpfung sind entscheidend für Produkt-, Prozess- und Geschäftsmodellinnovationen und bilden gleichzeitig die Grundlage für eine resilientere Forschungslandschaft.

Die Umsetzung datengestützter Forschungsprojekte in der iGW wird jedoch durch uneinheitliche rechtliche Anforderungen erschwert. Besonders betroffen sind klinische Studien sowie die Nutzung von Versorgungsdaten für Forschungszwecke. Divergierende rechtliche Vorgaben – etwa bei Einwilligungen, Rollenverteilungen oder Genehmigungsverfahren – sowie die unterschiedliche Auslegung zentraler Rechtsgrundlagen wie Art. 89 DSGVO oder § 27 BDSG führen zu Verzögerungen, erhöhtem Verwaltungsaufwand und ausbleibenden Investitionen. Deutschland gilt im internationalen Vergleich ohnehin als langsam beim Study Startup, was seine Wettbewerbsfähigkeit weiter schwächt. Eine zukunftsfähige und datenschutzkonforme Forschungslandschaft erfordert daher verlässliche rechtliche Rahmenbedingungen, praxisnahe Standards und einheitlich anerkannte Instrumente für Sekundärnutzung, Datenspende und internationale Kooperationen.

Zugang zu Forschungsdaten ermöglichen und absichern

Ein effektiver Datenschutzrahmen muss den Zugang zu Versorgungsdaten für wissenschaftliche Zwecke verlässlich ermöglichen – unabhängig von Trägerschaft, Standort oder Datenkategorie. Dafür braucht es eine klare rechtliche Grundlage für die dezentrale Nutzung medizinischer Daten und die ausdrückliche Anerkennung privatwirtschaftlicher Forschung im BDSG. Länder wie Dänemark oder Frankreich zeigen bereits, wie eine datenschutzkonforme und gleichzeitig forschungsfreundliche Datennutzung besser gelingen kann: Klare gesetzliche Rahmenbedingungen und zentrale Datenschutzstrukturen ermöglichen dort den verantwortungsvollen Zugang zu Gesundheitsdaten.

- ***Einheitliche Datenschutzregelungen für dezentrale Forschung schaffen:*** *Klinische Studien und die Nutzung von Real-World Data (RWD) erfordern eine bundeseinheitliche Auslegung und Anwendung des Datenschutzes. Landesspezifische Regelungen zum Gesundheitsdatenschutz müssen harmonisiert werden, um Kooperationen in der Patientenversorgung und medizinischen Forschung nicht unnötig zu erschweren. Dies gilt insbesondere für die Abgrenzung zwischen Versorgungsdaten (Daten, die im Rahmen der Behandlung entstehen und für Forschungszwecke sekundär genutzt werden können), primär erhobenen Forschungsdaten sowie allgemeinen Gesundheitsdaten im Sinne der DSGVO. Zudem braucht es rechtliche Vorgaben für die Sekundärnutzung bereits erhobener Versorgungsdaten zu Forschungszwecken, etwa im Rahmen von Registerstudien oder KI-*

basierten Analysen. Eine klare Abstimmung zwischen Bund und Ländern ist notwendig, um einheitliche, ermöglichende Maßstäbe für die Weitergabe und Nutzung medizinischer Daten zu schaffen.

- ***Forschungsgleichstellung im BDSG auch für privatwirtschaftliche Forschung verankern**: Das Bundesdatenschutzgesetz (BDSG) sollte eindeutig festhalten, dass auch privatwirtschaftlich durchgeführte- oder finanzierte Projekte unter den Begriff der Forschung fallen. Trotz der im GDNG enthaltenen Öffnungsklauseln fehlt bislang eine eindeutige gesetzliche Verankerung. Diese gesetzliche Klarstellung ist jedoch erforderlich, um Forschungsvorhaben unabhängig von ihrer Trägerschaft gleichzustellen und Investitionen in datenbasierte Innovationen in Deutschland abzusichern.*

Datenschutzrechtliche Rahmenbedingungen für Gesundheitsforschung vereinheitlichen

Klinische Prüfungen erfordern die Zusammenarbeit mehrerer Beteiligter, darunter der Sponsor (z. B. aus der Industrie), das Prüfzentrum (z. B. eine Klinik) und für unterstützende Aufgaben die Clinical Research Organization (CRO). Allerdings besteht Uneinigkeit darüber, welche datenschutzrechtlichen Verträge zwischen diesen Parteien erforderlich sind. In der Regel gilt der Sponsor als Verantwortlicher, da er den Prüfplan erstellt und genehmigen muss – oft in Abstimmung mit der CRO.

Auch das sogenannte „Forschungsprivileg“ (Art. 89 DSGVO bzw. § 27 BDSG) wird von Prüfzentren und Ethikkommissionen unterschiedlich interpretiert. So wird häufig eine separate Einwilligung für die Sekundärforschung verlangt. Die rechtliche Bewertung datenschutzrechtlicher Verantwortlichkeiten variiert erheblich – je nach EU-Land, Bundesland und sogar innerhalb einzelner Ethikkommissionen; je nach EU-Land wird beispielsweise dieselbe Studienstruktur unterschiedlich bewertet – mal als gemeinsame, mal als getrennte Verantwortlichkeit. Auch innerhalb Deutschlands gibt es keine einheitliche Praxis: Während einige Ethikkommissionen bestimmte Formulierungen in den Informed Consent Forms (ICF) als kritisch ansehen, verlangen andere genau diese Inhalte als notwendig. Dies führt dazu, dass identische Forschungsprojekte je nach Standort unterschiedlichen vertraglichen, ethischen und datenschutzrechtlichen Anforderungen unterliegen, was die Planung, Genehmigung und Durchführung erheblich verkompliziert.

- ***Rechtssicherheit für die Sekundärnutzung von Forschungsdaten schaffen**: Die unterschiedliche Auslegung des „Forschungsprivilegs“ nach Art. 89 DSGVO bzw. § 27 BDSG führt dazu, dass manche Prüfzentren eine zusätzliche Einwilligung für die Sekundärforschung verlangen. Hier sind bundeseinheitliche Vorgaben nötig, um mehr Planungssicherheit für Forschende zu gewährleisten und unnötige Verzögerungen zu vermeiden. Hilfreich wären zudem zentrale „Shared Best Practice“-Informationen und kurze Tutorials, da viele Anträge derzeit wegen kleinerer Mängel oder fehlender Angaben zurückgewiesen werden, was den Genehmigungsprozess verzögert.*
- ***Verantwortlichkeiten in der Forschung datenschutzkonform definieren**: Die Einstufung als gemeinsame oder getrennte Verantwortlichkeit variiert nicht nur zwischen EU-Ländern, sondern auch innerhalb Deutschlands. Diese Unklarheit erschwert Vertragsverhandlungen und verlängert den Prozess bis zum Studienstart. Eine einheitliche Definition der Verantwortlichkeiten durch die Datenschutzbehörden könnte hier Abhilfe schaffen.*

Datenschutzkompetenz stärken und Orientierung geben

Der Zugang zu qualifizierter Datenschutzexpertise ist ein zentraler Erfolgsfaktor für Forschungsvorhaben. In der Praxis fehlt es jedoch häufig an internem Know-how – insbesondere bei extern bestellten Datenschutzbeauftragten. Gleichzeitig fehlen verbindliche Orientierungshilfen, die Kliniken und Prüfzentren bei der rechtlichen Einordnung zentraler Fragen unterstützt. Gerade bei bundeslandübergreifenden Forschungsprojekten muss mit verschiedenen landesspezifischen Regelungen gearbeitet werden, was die Komplexität zusätzlich erhöht. Zudem werden in den Krankenhäusern zu wenig Ressourcen bereitgestellt, um Forschungsvorhaben durch in Datenschutzfragen geschultes Personal zu

begleiten. Dies wird insbesondere bei Einwilligungsfragen deutlich. Unklar ist häufig, wie konkret Einwilligungen zur Nutzung personenbezogener Daten für wissenschaftliche Forschung ausgestaltet sein müssen. Dies führt regelmäßig dazu, dass zahlreiche hochqualitative Daten nicht weiterverwendet werden können, weil die Einwilligung bei der Datenerhebung so konkret ausgestaltet wurde, dass sie nur für einen ganz bestimmten Verwendungszweck / Anwendungsfall gilt.

- ***Praxisnahe Orientierungshilfe durch die Datenschutzkonferenz (DSK) bereitstellen****: Datenschutzvorgaben werden von Ethik-Kommissionen und Kliniken häufig restriktiv ausgelegt, um DSGVO-Verstöße zu vermeiden. Das hat zur Folge, dass sich Forschungsprojekte verzögern oder gar nicht in Deutschland durchgeführt werden. Um Rechtsunsicherheiten zu verringern und den Abstimmungsaufwand zu reduzieren, sollte die DSK eine bundeseinheitliche Orientierungshilfe mit praxisnahen Empfehlungen bereitstellen. In Anlehnung an das RACOON Best-Practice-Papier könnte diese Orientierungshilfe Fallbeispiele, Checklisten, Mustervorlagen und die datenschutzrechtliche Einordnung typischer Nutzungsszenarien enthalten – etwa zur Sekundärnutzung von Versorgungsdaten oder zum Einsatz lernender Systeme im Klinikbetrieb. Sie sollte die häufigsten Problemfelder in klinischen Prüfungen adressieren, darunter die Anforderungen an ICFs, Broad Consent und Datenschutzregelungen bei Forschungsdaten. Ziel ist ein bundesweit anerkannter Datenschutzrahmen, der allen Beteiligten – Ethik-Kommissionen, Prüfzentren, Forschungseinrichtungen und Industrie – klare und rechtssichere Handlungsgrundlagen bietet und die Möglichkeiten der DSGVO ausschöpft.*
- ***Zuständigkeit von Ethik-Kommissionen im Datenschutz abgrenzen:*** *Das Rollenverständnis von Ethik-Kommissionen sollte bundesweit geschärft und klar von datenschutzrechtlichen Prüfaufgaben abgegrenzt werden, so wie es die Handreichung des Arbeitskreises medizinischer Ethik-Kommissionen vorsieht. Um zusätzliche Hürden im Genehmigungsverfahren zu vermeiden, sollten sich Ethik-Kommissionen auf ihre ethische Kernaufgabe konzentrieren und datenschutzrechtliche Bewertungen ausschließlich im Rahmen dieser Handreichung vornehmen.*

Einwilligungsprozesse und Datenspende verständlich und rechtssicher gestalten

Einwilligungsdokumente wie ICF variieren stark in Aufbau, Länge und Detailtiefe. Bei multinationalen klinischen Prüfungen muss die ICF häufig speziell für Deutschland angepasst werden. Zudem variieren die vertraglichen Anforderungen je nach Bundesland, da Prüfzentren und Ethik-Kommissionen unterschiedliche Auffassungen vertreten. Betroffene müssen häufig zwei separate Einwilligungen abgeben – eine für die Studienteilnahme, eine für die Begleitforschung. Gleichzeitig werden die ICFs immer umfangreicher und für Patientinnen und Patienten schwer verständlich. Der Datenschutz nimmt dabei den größten Teil ein. In der Praxis ist es kaum möglich, die relevanten Dokumente wie ICFs, Studienverträge oder CMO-Dokumente konsistent zu halten.

Die DSGVO (Erwägungsgrund 33) eröffnet die Möglichkeit eines Broad Consent – also einer einmaligen Zustimmung zur Datennutzung in bestimmten Forschungsfeldern. Diese Option wird in Deutschland bislang uneinheitlich anerkannt. Klare Vorgaben würden langfristige Forschung erleichtern und rechtliche Unsicherheiten bei Studienplanung und Einwilligungsprozessen vermeiden. Auch zur Datenspende fehlen bundeseinheitliche Standards. Zudem besteht Unklarheit darüber, wie konkret Einwilligungen für wissenschaftliche Forschung ausgestaltet sein müssen. Gerade bei langfristigen Studien oder bei der Einwilligung nicht einwilligungsfähiger Personen – etwa in der Demenzforschung – sind praxistaugliche, flexible Lösungen erforderlich.

- ***Rechtssicheren Broad Consent als Standard verankern****: Ein Broad Consent ermöglicht eine einmalige, allgemeine Zustimmung zur Datennutzung für künftige Forschungsvorhaben in bestimmten Forschungsbereichen. Während dieses Konzept in anderen Ländern bereits anerkannt ist, bestehen in Deutschland weiterhin Unsicherheiten. Eine rechtssichere Ausgestaltung des Broad Consent*

würde langfristige Forschungsprojekte erleichtern und dabei den Patientinnen und Patienten die Möglichkeit geben, eine bewusste Entscheidung zu treffen. Es muss auch klargestellt werden, dass der Broad Consent der Medizininformatik-Initiative nur eine Ausgestaltung dieses Konzepts ist und auch anders gefasste Broad Consent Erklärungen rechtskonform ausgestaltet werden können.

- ***Einheitliche Vorgaben für die Datenspende zur freiwilligen Sekundärdatennutzung schaffen:*** *Für die freiwillige Datenspende zur Sekundärnutzung von Versorgungsdaten (im Sinne eines Broad Consent) fehlen bislang bundeseinheitliche und rechtssichere Vorgaben. Aktuell erstellt jeder Akteur eigene Versionen mit unterschiedlichen Pflichtangaben und Hinweisen, was die Verständlichkeit und eine rechtskonforme Nutzung für Patientinnen und Patienten erschwert. Erforderlich ist eine gesetzlich vorgegebene und möglichst kompakte Formulierung der Datenspende-Erklärung innerhalb der Patienteneinverständniserklärung, die verbindlich von allen Behörden und Ethik-Kommissionen anerkannt wird. Eine Orientierung an zentralen Datenschutzstandards – etwa aus klinischen Prüfungen – könnte helfen, Redundanzen zu vermeiden und Prozesse zu vereinfachen. Dabei muss eindeutig abgegrenzt werden, wie sich die Datenspende juristisch und prozesstechnisch von der klassischen informierten Einwilligung (Informed Consent) sowie vom Broad Consent unterscheidet. Gleichzeitig sollte die Datenspende so ausgestaltet sein, dass eine datenschutzkonforme Rückkontaktierung ermöglicht wird, etwa bei relevanten Erkenntnissen aus klinischen Studien.*
- ***Bundeseinheitliche Einwilligungsformulare für klinische Studien etablieren:*** *Die Unterschiede zwischen den Bundesländern und Ethik-Kommissionen führen zu erheblichem Mehraufwand. Eine bundesweit einheitliche ICF-Vorlage mit praxisgerechten Vorgaben zu Datenschutzaspekten könnte die administrative Last für Prüfzentren und Sponsoren deutlich reduzieren. Zudem sollte die Verständlichkeit der ICF für Patientinnen und Patienten verbessert werden, um deren informierte Entscheidung zu erleichtern. Dazu gehört auch die Verkürzung des ICF auf eine praxistaugliche Länge ggfs. unterstützt durch audiovisuelle Begleitmaterialien.*
- ***Einwilligungen beim internationalen Datentransfer rechtssicher ermöglichen:*** *Unternehmen holen bereits zum Zeitpunkt der Kooperation die Einwilligungen für eine mögliche internationale Datenweitergabe ein. Da zu diesem frühen Zeitpunkt jedoch oft unklar ist, in welchen Ländern beispielsweise Zulassungs- oder Erstattungsverfahren (Market Access Approvals) beantragt werden, besteht das Risiko, dass die Einwilligung später nicht als wirksam anerkannt wird. Hier sind rechtssichere Lösungen notwendig, damit Unternehmen die erhobenen Daten insbesondere auch bei Zulassungsprozessen außerhalb der EU verwenden können.*

Rechtssicherheit bei Anonymisierung und Pseudonymisierung schaffen

Eine belastbare rechtliche Grundlage für die Verarbeitung anonymisierter und pseudonymisierter Gesundheitsdaten ist unverzichtbar für datengestützte Forschung und Entwicklung. Die ausgedehnte Auslegung des Begriffs der personenbezogenen Daten durch Rechtsprechung und Aufsichtsbehörden erschwert die Nutzung vorhandener Gesundheitsdaten erheblich. Die DSGVO enthält weder eine Legaldefinition von „Anonymisierung“ noch einen Mindeststandard, der unabhängig vom Forschungsgegenstand vorgibt, ab wann die Identifizierbarkeit ausgeschlossen ist. Ebenso fehlen praxistaugliche Vorgaben für eine dauerhafte Pseudonymisierung – insbesondere bei älteren Bestandsdaten, für die keine Einwilligung nach heutigen Standards vorliegt. Dies erschwert nicht nur die Nutzung bestehender Datenbestände, sondern auch die vertragliche Ausgestaltung von Auftragsverarbeitungen.

Besonders große Unsicherheit besteht bei der Frage, wann Bilddaten als anonymisiert gelten können. Erwägungsgrund 26 der DSGVO sieht vor, dass die Wahrscheinlichkeit einer Re-Identifikation sowie der damit verbundene Aufwand zu berücksichtigen sind. Begriffe wie „Wahrscheinlichkeit“ und „Verhältnismäßigkeit“ lassen jedoch einen großen Ermessensspielraum zu, was zu erheblich abweichenden Bewertungen durch die Landesaufsichtsbehörden führt. Ähnliche Herausforderungen bestehen auch mit Biomaterialen bzw. Bio-Samples, wobei unklar bleibt, ob sie als Daten oder lediglich als Träger von Daten zu klassifizieren sind. In dem Zusammenhang sollte geprüft werden, ob ein Re-Identifizierungsversuch ohne Erlaubnistatbestand strafrechtliche Konsequenzen nach sich ziehen sollte.

Im Rahmen einer Auftragsverarbeitung können Daten aus Sicht des Verarbeiters anonym sein – etwa, wenn er faktisch oder rechtlich nicht in der Lage ist, eine betroffene Person zu identifizieren. In diesen Fällen unterliegen die Daten nicht den datenschutzrechtlichen Anforderungen der DSGVO. Die Aufsichtsbehörden hingegen verfolgen häufig einen absoluten Ansatz[1], dem zufolge Daten so lang als personenbezogen gelten, wie irgendeine Möglichkeit zur Re-Identifikation besteht – unabhängig davon, ob der konkrete Verarbeiter dazu faktisch oder rechtlich in der Lage ist. Diese Auslegung erschwert die Umsetzung datenschutzkonformer Prozesse und belastet insbesondere die Vertragsgestaltung. Der absolute Ansatz steht dabei im Widerspruch zur Rechtsprechung des EuGH, der zuletzt einen subjektiven Ansatz verfolgte (vgl. Breyer, C-582/14 vom 19.10.2016 sowie zuletzt auch EuG, SRB./.EDSB, T-557/20 vom 26.04.2023). Außerdem erschweren strenge Datenschutzvorgaben oftmals die Nutzung großer pseudonymisierter Datensätze, insbesondere wenn sie vor dem Inkrafttreten der DSGVO erhoben wurden. Da für diese älteren Daten oft keine expliziten Einwilligungen nach den heutigen Standards vorliegen, wird aus Vorsicht häufig auf diese Daten verzichtet, obwohl sie für Forschungszwecke wertvoll wären.

Datenschutzkonforme Standards für Anonymisierung und Pseudonymisierung definieren

Um die bestehende Rechtsunsicherheit zu beheben, braucht es konkret anwendbare Kriterien und bundeseinheitlich anerkannte Verfahren. Insbesondere für die Bewertung von Re-Identifizierbarkeiten, den Umgang mit historischen Datenbeständen sowie die Vertragsgestaltung im Rahmen von Auftragsverarbeitungen bestehen erhebliche Unsicherheiten. Hier braucht es einheitliche Standards und praxistaugliche Leitlinien, um die datenschutzkonforme Nutzung von Gesundheitsdaten zu ermöglichen und administrative Aufwände zu reduzieren. Diese Standards sollten unter Berücksichtigung des zu erwartenden SRB-Urteils des EuGH und in Abstimmung mit den angekündigten Leitlinien zur Anonymisierung durch den Europäischen Datenschutzausschuss entwickelt werden. Darüber hinaus sollten auch Maßgaben für ein DSGVO-konformes Training von KI-Modellen (z. B. Input-Output-Kontrollen) definiert werden – insbesondere mit Blick auf mögliche Rechtsgrundlagen, die ein Training von KI mit Gesundheitsdaten im Einklang mit Art. 9 DSGVO ermöglichen.

- ***Verlässliche Vorgaben zur Entpersonalisierung medizinischer Daten schaffen – auch für spezifische Datenkategorien:*** *Es braucht klare gesetzliche Vorgaben und technische Standards, die definieren, ab wann personenbezogene (Gesundheits-)Daten als anonymisiert gelten. Zudem muss klargestellt werden, wie pseudonymisierte Daten langfristig verknüpfbar bleiben können – etwa durch die Verwendung stabiler Pseudonyme, bei denen die verarbeitende Stelle keine Re-Identifikation vornehmen kann. Dabei sollten auch die bestehenden Leitlinien zur Pseudonymisierung, insbesondere mit Blick auf die Leitlinien 1/2025, deutlich praxistauglicher ausgestaltet werden. Einheitliche Regelungen braucht es auch zur Anonymisierung und Pseudonymisierung von spezifischen Bildkategorien wie Bilddaten – insbesondere zur Frage, welcher Aufwand zur Re-Identifikation als verhältnismäßig sicher eingestuft wird. Ergänzend ist zu klären, inwieweit biologische Proben (Bio-Samples) als anonymisiert gelten, obwohl ein DNA-Rückschluss theoretisch immer möglich ist. Entscheidend ist hier eine einheitliche Bewertung durch die Landesdatenschutzbehörden. Die DSK sollte dazu einen bundesweit gültigen technischen Anonymisierungsleitfaden mit Fallbeispielen als Orientierungshilfe vorlegen, um die Bewertung für Unternehmen und Forschungseinrichtungen zu erleichtern. Langfristig sollte dieser auch auf europäischer Ebene harmonisiert werden, damit eine in Deutschland anerkannte Anonymisierung auch in anderen DSGVO-Mitgliedstaaten gilt.*

[1] *Beim „absoluten Ansatz" gelten Daten als personenbezogen, sobald irgendeine Stelle eine Re-Identifikation vornehmen könnte – unabhängig davon, ob der konkrete Verarbeiter dazu tatsächlich in der Lage ist.*

- ***Anonymitätsbewertung an tatsächlicher Re-Identifizierbarkeit ausrichten:*** *Die Beurteilung der Anonymität von Gesundheitsdaten sollte sich an den tatsächlichen Zugriffsmöglichkeiten der Datenverarbeiter orientieren. Die Anforderungen an eine Anonymisierung dürfen nicht pauschal überhöht sein. Denkbar wäre eine gesetzlich verankerte Vermutungsregel – etwa nach dem Vorbild der US-amerikanischen HIPAA-Regelungen (Health Insurance Portability and Accountability Acts) – die festlegt, wann Daten als hinreichend anonym gelten. Alternativ sollte der Gesetzgeber eine eigene Rechtsgrundlage für die Anonymisierung medizinischer Daten schaffen, um bestehende Unsicherheiten zu beseitigen.*
- ***Pseudonymisierte Bestandsdaten rechtssicher nutzbar machen:*** *Die strengen Vorgaben zur Nutzung von Daten, die vor dem Inkrafttreten der DSGVO am 25. Mai 2018 erhoben wurden, führen zu Einschränkungen. Es sollte ein gesetzlich verankerter Mechanismus geschaffen werden, der es ermöglicht, Bestandsdaten unter bestimmten Schutzvorkehrungen weiterhin für Forschungszwecke zu nutzen, ohne dass eine nachträgliche Einwilligung erforderlich ist. Insbesondere für epidemiologische Studien und die Entwicklung KI-gestützter Verfahren, die auf longitudinalen Datensätzen beruhen, sind solche historischen Datensätze essenziell.*
- ***Zugang zu anonymisierten Behandlungsdaten für die Forschung ermöglichen****: Die gesetzlich geregelte Nutzung anonymisierter Behandlungsdaten durch alle forschenden Akteure – einschließlich der Industrie – muss unter Beachtung eines klaren Datenschutzregimes ermöglicht werden. Diese Daten sind essenziell für die medizinische Forschung und Nutzenbewertung in Deutschland. Das GDNG schafft hierfür bereits eine erste wichtige Grundlage, sollte jedoch weiterentwickelt werden, um einen effektiven und rechtssicheren Zugang zu gewährleisten. Insbesondere für den Einsatz von KI ist eine Abgrenzung erforderlich, welche Datenmodelle als anonymisierte Daten einzuordnen sind. So erscheint es sinnvoll, Bilddaten, die prima vista durch Aufnahmen von außen zustande kommen z. B. Fotografien der Haut / Zähne von Bilddaten zu unterscheiden, deren Zuordnung sich dem menschlichen Auge verschließen – z. B. histologische Schnitte oder endoskopische Befunde.*

Datenschutzgerechte Integration digitaler Versorgungslösungen sicherstellen

Auch außerhalb klassischer Forschung entstehen im Versorgungskontext zunehmend große, datenschutzrechtlich relevante Datenmengen – etwa durch robotische Assistenzsysteme, KI-gestützte Entscheidungsunterstützung oder vernetzte Medizintechnik. Diese Anwendungen erfordern eine zentrale Verarbeitung von Behandlungsdaten, die über einrichtungs- und länderübergreifende Grenzen hinausgeht. Gleichzeitig fehlt es an bundeseinheitlichen Vorgaben, wie digitale MedTech-Systeme datenschutzkonform betrieben und weiterentwickelt werden können. Besonders die föderale Zersplitterung – etwa in den Landeskrankenhausgesetzen – erschwert die flächendeckende Einführung digitaler Anwendungen in der Regelversorgung.

Die Installation und der Betrieb dieser Anwendungen müssen in jedem Bundesland separat geprüft, bewertet und vertraglich geregelt werden. Diese Prozesse binden personelle und finanzielle Ressourcen und bremsen Innovationen aus. Hinzu kommt: Viele dieser Technologien basieren auf dem Abgleich bereits vorhandener Datensätze – etwa, um mithilfe von KI Hinweise zur besseren Durchführung von Prozeduren zu geben. Zwar ermöglicht das GDNG bereits in bestimmten Fällen die Sekundärnutzung von Versorgungsdaten, jedoch bleibt die Nutzung lokaler Krankenhausdaten für klinikinterne Anwendungen weiterhin durch die Heterogenität landesrechtlicher Vorgaben erschwert. Im Zuge der Krankenhausreform bietet sich daher ein konkretes Zeitfenster, die datenschutzrechtlichen Regelungen in den Landeskrankenhausgesetzen bundesweit zu vereinheitlichen. Dies würde sowohl die Einführung innovativer Versorgungslösungen erleichtern als auch deren Weiterentwicklung durch privatwirtschaftliche Anbieter ermöglichen – bei gleichzeitiger Wahrung der Patientenrechte.

- ***Nutzung digitaler Behandlungsdaten bundesweit ermöglichen:*** *Der Einsatz innovativer digitaler Systeme in der Patientenversorgung wie robotische Assistenzsysteme oder KI-gestützte Entscheidungsunterstützung setzt voraus, dass Behandlungsdaten zentral verarbeitet werden dürfen. Dafür braucht es einheitliche Datenschutzregelungen, die eine rechtssichere und länderübergreifende Anwendung ermöglichen. Die datenschutzrechtliche Differenzierung zwischen Forschung und Versorgung darf dabei technologischen Fortschritt in der klinischen Anwendung nicht ausbremsen.*
- ***Datenschutz im Rahmen der Krankenhausreform harmonisieren:*** *Im Zuge der geplanten Krankenhausreform bietet sich die Chance, die heterogenen datenschutzrechtlichen Regelungen in den Landeskrankenhausgesetzen zu harmonisieren. Dies würde sowohl die Implementierung innovativer Versorgungslösungen als auch deren Weiterentwicklung durch privatwirtschaftliche Akteure erleichtern – bei gleichzeitiger Wahrung der Patientenrechte und gleichzeitiger Stärkung des Patientennutzens.*

Datennutzung innerhalb von Trägerstrukturen rechtssicher ermöglichen

Die zunehmende Digitalisierung der Versorgung bringt auch innerhalb von Krankenhausträgern neue datenschutzrechtliche Herausforderungen mit sich. So dürfen beispielsweise Mitarbeitende eines Medizinischen Versorgungszentrums (MVZ) nicht ohne Weiteres auf Patientendaten eines Krankenhauses zugreifen – auch dann nicht, wenn beide Einrichtungen zum gleichen Träger gehören und sich im selben Gebäude befinden. Die bislang restriktive Trennung der datenschutzrechtlichen Verantwortlichkeiten verhindert eine einheitliche Datenverarbeitung und führt zu vermeidbaren Informationsbrüchen. Dies beeinträchtigt nicht nur die Versorgungsqualität, sondern erschwert auch die Umsetzung innovativer, einrichtungsübergreifender Versorgungsmodelle, die direkten Patientennutzen versprechen.

- ***Datennutzung innerhalb eines Trägers einheitlich regeln:*** *Um eine kontinuierliche, koordinierte Versorgung sicherzustellen, sollte der datenschutzkonforme Zugriff auf Patientendaten innerhalb einer Trägerstruktur – etwa zwischen Krankenhaus und MVZ – unter klaren Voraussetzungen zulässig sein. Dazu braucht es eine bundesweit einheitliche Regelung, wann von einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit ausgegangen werden kann und wie technische Schutzmaßnahmen (z. B. Mandantentrennung) praxistauglich umgesetzt werden können. Die bisherige restriktive Trennung zwischen Einrichtungen desselben Trägers erschwert intersektorale Zusammenarbeit und führt zu Qualitätseinbußen in der Versorgung.*

Internationale Datennutzung und europäische Anschlussfähigkeit sichern

Die Wettbewerbsfähigkeit der iGW hängt zunehmend davon ab, wie verlässlich und rechtskonform Gesundheitsdaten über Ländergrenzen hinweg genutzt werden können. Die uneinheitliche datenschutzrechtliche Auslegung – sowohl innerhalb Deutschlands als auch zwischen den EU-Mitgliedstaaten – erschwert die grenzüberschreitende Nutzung und gefährdet die Anschlussfähigkeit deutscher Unternehmen an internationale Datenräume, Forschungsverbünde und Digitalinfrastrukturen.

Die Einbindung von leistungsfähigen Technologieanbietern mit Sitz oder Verbindung außerhalb der EU wird von den Datenschutzbehörden kritisch bewertet – bereits eine Beteiligung durch eine US-Muttergesellschaft kann aus Sicht vieler Behörden als problematisch gelten. Häufige Bedenken betreffen mögliche Drittstaatentransfers gemäß Art. 45 ff. DSGVO, insbesondere aufgrund potenzieller Zugriffsberechtigungen durch ausländische Behörden.

Rechtsklarheit für internationalen Datentransfer schaffen: *Es braucht verbindliche und praktikable Regelungen für den internationalen Datenaustausch – sowohl mit ausländischen Zulassungsbehörden wie der FDA (U.S. Food and Drug Administration) als auch im Umgang mit Cloud-Dienstleistern. Insbesondere Angemessenheitsbeschlüsse für Drittstaaten, in denen zentrale Handels- und Geschäftspartner sitzen, wären ein entscheidender Schritt, um internationale Projekte rechtssicher und praktikabel zu gestalten.*

- ***Studiendaten rechtssicher für internationale Zulassungszwecke nutzbar machen:*** *Für die internationale Zulassung medizinischer Produkte müssen personenbezogene Studiendaten an Zulassungsbehörden außerhalb der EU übermittelt werden. Da hierfür meist kein EU-Angemessenheitsbeschluss gilt und Standardvertragsklauseln mit Behörden nicht anwendbar sind, bleibt oft nur die Einwilligung der Betroffenen. Diese ist jedoch rechtlich unsicher und in der Praxis schwer umsetzbar, etwa weil nicht alle Zielstaaten zum Zeitpunkt der Einwilligung feststehen oder der komplexe Sachverhalt für Patientinnen und Patienten schwer verständlich ist. Es braucht daher eine DSGVO-konforme Klarstellung oder Ergänzung, dass solche Zulassungsverfahren unter die Ausnahmen des Art. 49 DSGVO fallen – um die Wettbewerbsfähigkeit des Studienstandorts Deutschland zu sichern.*
- ***Einsatz von US-Dienstleistern datenschutzkonform ermöglichen****: Es muss geregelt werden, ob bereits die bloße Möglichkeit eines Zugriffs durch US-Behörden auf Rechenzentren in Europa als tatsächlicher Drittstaatentransfer in die USA gewertet wird. Obwohl das Problem durch den Angemessenheitsbeschluss zum EU-US Data Privacy Framework vom 10. Juli 2023 an Bedeutung verloren hat, sollte die restriktive Auslegungspraxis grundsätzlich überdacht werden. Eine praxisgerechte Bewertung, die auch weitere Umstände wie z. B. eine Pseudonymisierung von Daten praxisgerechter miteinbezieht, könnte Unternehmen mehr Handlungsspielraum geben.*

Europäische Gesundheitsdateninfrastruktur aktiv mitgestalten

Nationale Sonderwege und fehlende Interoperabilität bremsen nicht nur die Verwertung von Innovationen aus, sondern gefährden auch die aktive Beteiligung an europäischen Vorhaben wie dem European Health Data Space (EHDS). Um die Anschlussfähigkeit deutscher Forschungseinrichtungen und Unternehmen zu sichern, braucht es eine frühzeitige und industriekompatible Ausgestaltung der Rahmenbedingungen auf europäischer und nationaler Ebene.

- ***Anschlussfähigkeit an den EHDS durch nationale Harmonisierung sicherstellen:*** *Deutschland sollte die Umsetzung des EHDS aktiv mitgestalten und bestehende nationale Blockaden abbauen – insbesondere durch eine Harmonisierung datenschutzrechtlicher Vorgaben und verbindliche Interoperabilitätsstandards. Dabei ist es zentral, nicht nur europäische Vorgaben umzusetzen, sondern auch die innerdeutsche Fragmentierung – etwa zwischen Bundesländern und konfessionellen Trägern – zu überwinden. Nur so lassen sich Zugangsbarrieren vermeiden, skalierbare digitale Projekte ermöglichen und die grenzüberschreitende Nutzung gemeinsamer europäischer Datenräume gewährleisten. Zugleich muss sichergestellt werden, dass auch eine parallele oder darüberhinausgehende Datennutzung außerhalb des EHDS rechtlich abgesichert bleibt.*
- ***Industriekompatible Datenzugangsverfahren schaffen:*** *Um die Beteiligung der Industrie am EHDS zu ermöglichen, braucht es transparente und praktikable Zugangsprozesse – sowohl für EHDS-Zugangsstellen (Health Data Access Bodies, HDABs) als auch für nationale Datenzugänge nach GDNG. Diese Verfahren sollten nicht ausschließlich forschungsbezogenen Akteuren vorbehalten sein, sondern auch privatwirtschaftliche Anwendungsfälle ermöglichen – z. B. für klinische Studien, Versorgungsforschung, KI-Entwicklung sowie Workflow- und Prozessoptimierungen.*

Über den BDI

Der BDI transportiert die Interessen der deutschen Industrie an die politisch Verantwortlichen. Damit unterstützt er die Unternehmen im globalen Wettbewerb. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen. Der BDI sorgt für die politische Flankierung internationaler Markterschließung und er bietet Informationen und wirtschaftspolitische Beratung für alle industrierelevanten Themen. Der BDI ist die Spitzenorganisation der deutschen Industrie und der industrienahen Dienstleister. Er spricht für 39 Branchenverbände und mehr als 100.000 Unternehmen mit rund acht Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Lobbyregisternummer: R000534

Redaktion
Rabea Knorr
Leiterin Abteilung Industrielle Gesundheitswirtschaft
T: +49 30 2028-1495
r.knorr@bdi.eu

Maria Kusmina
Stellvertretende Leiterin Abteilung Industrielle Gesundheitswirtschaft
T: +49 30 2028-1505
m.kusmina@bdi.eu

Dr. Michael Dose
Referent Digitalisierung und Innovation
T: +49 30 2028-1560
m.dose@bdi.eu

BDI Dokumentennummer: D2069