



Sicher, vertrauenswürdig und dezentral

# WIE DATENRÄUME HELFFEN, NEUE GESCHÄFTSMODELLE ZU ENTWICKELN

In der heutigen Zeit werden sehr große Datenmengen generiert und verwaltet, dennoch wird der Wert der Daten in Deutschland und Europa nicht voll ausgeschöpft. Die gemeinsame Nutzung von Daten kann und soll datengetriebene Anwendungen noch weiter vorantreiben, bei der Erfüllung regulatorischer Anforderungen helfen sowie einen finanziellen Mehrwert für Firmen schaffen. Viele kleine und mittlere Unternehmen zögern derzeit jedoch, Daten untereinander auszutauschen, weil sie befürchten, die Hoheit über ihre Daten zu verlieren und nicht wissen, wer Zugriff auf sie hat und wofür die Daten verwendet werden<sup>[1]</sup>.

**M**ithilfe von Datenräumen können Unternehmen und Organisationen Informationen und damit verbundene Dienste sicher austauschen und nutzen. Voraussetzung für den Betrieb eines Datenraums ist ein rechtlicher und technischer Standard.

Erste Konzepte für Datenräume gibt es in der Informatik bereits seit 15 Jahren. Der Begriff „Datenraum“ bezieht sich auf eine Art Datenbeziehung zwischen vertrauenswürdigen Partnern, die sich an die gleichen Standards und Richtlinien für die Speicherung und den Austausch von Daten halten. Ein entscheidender Aspekt des Konzepts ist jedoch, dass die Daten nicht zentral, sondern an der Quelle gespeichert und nur bei Bedarf übertragen werden. Ein Datenraum ist die Summe aller seiner Teilnehmer, die Datenanbieter, Nutzer und Vermittler sein können.

Die Forschung des Fraunhofer ISST führte diese Idee weiter und gipfelte 2015 in der Gründung der International Data Spaces Association und der Entwicklung erster Konzepte und Standards für Datenräume.

## GAIA-X-PROJEKT

Gaia-X geht noch einen Schritt weiter als das Datenraumkonzept und berücksichtigt gängige datenbezogene Dienste wie Speicher und Webserver, um Interoperabilität zwischen verschiedenen Cloud-Anbietern und IT-Infrastrukturen herzustellen. Dabei ist Ziel des Gaia-X-Projektes, einen Rahmen zu schaffen, der es allen Beteiligten aus unterschiedlichen Branchen ermöglicht, sich auf ein einheitliches Regelwerk und die Einhaltung von gemeinsamen Grundwerten im Datenraum zu einigen. Grundlegende Werte sind: Datensouveränität, Datenschutz, Vertraulichkeit, IT-Sicherheit, Technologieneutralität und Interoperabilität. Für die Cybersicherheit besteht die Mindestanforderung darin, die Anforderungen des European Cybersecurity Scheme-Basic Level der European Union Agency for Cybersecurity (ENISA) zu erfüllen<sup>[1]</sup>.

Es gibt drei Anforderungsstufen (European Cybersecurity Scheme): Basic Level, Substantial Level, High Level. Jedes Level wird durch das Cyber-Sicherheitsframework der ENISA kontrolliert. Gaia-X hat sich zu einer europäischen Initiative entwickelt, die Spezifikationen des Gaia-X-

Frameworks veröffentlicht und Softwareprogramme zur Einhaltung des Frameworks zur Verfügung stellt. Alle Ressourcen stehen unter einer Open-Source-Lizenz und können daher von jedem genutzt werden.

## BESTANDTEILE EINER DATENRAUMLÖSUNG

Eine Datenraumlösung kann aus verschiedenen Systemelementen, Systemkomponenten und Teilnehmern bestehen.

Der Datenraum selbst wird als eine Sammlung von Systemkomponenten definiert und verwendet, die für den sicheren Austausch von Daten und Diensten erforderlich sind. Verschiedene Datenräume können innerhalb eines Dienstes regelkonform koexistieren.

Neben dem Datenraum spielen die Teilnehmer eine entscheidende Rolle:

- Der Anbieter ist eine Person oder Institution, die Daten im Datenraum anbietet.
- Der Konsument ist jene Partei, die Daten erwerben möchte<sup>[1]</sup>.

Um die Systemelemente zu validieren und die Interoperabilität zu gewährleisten, werden Compliance-Services eingesetzt. Damit sich Anbieter und Konsument am Datenraum anmelden können, werden Identity-Services benötigt. Ein Katalog listet alle in einem Datenraum angebotenen Daten auf. In diesem Verzeichnis können Anbieter ihre Daten veröffentlichen und Konsumenten nach verfügbaren Angeboten suchen. Für den Datenaustausch stehen Dienste zur Verfügung, die die Transaktion zwischen Anbieter und Konsument unterstützen, einschließlich Vertragsabschluss, Registrierung und Datenübertragung.

Ein Datenraum kann ergänzende Systemkomponenten enthalten, die den Benutzerkomfort erhöhen und in bestimmten Bereichen zusätzliche Funktionen bieten. So ist ein Webportal ein wesentliches Systemelement, das einen benutzerfreundlichen Zugang zu einem Datenraum ermöglicht. Dazu gehört der einfache Zugriff auf die Konten der Teilnehmer sowie die Bereitstellung und Nutzung von datenrauminternen Diensten. Heutige Datenräume bieten neben aktuellen IT-Sicherheitsstandards und den oben

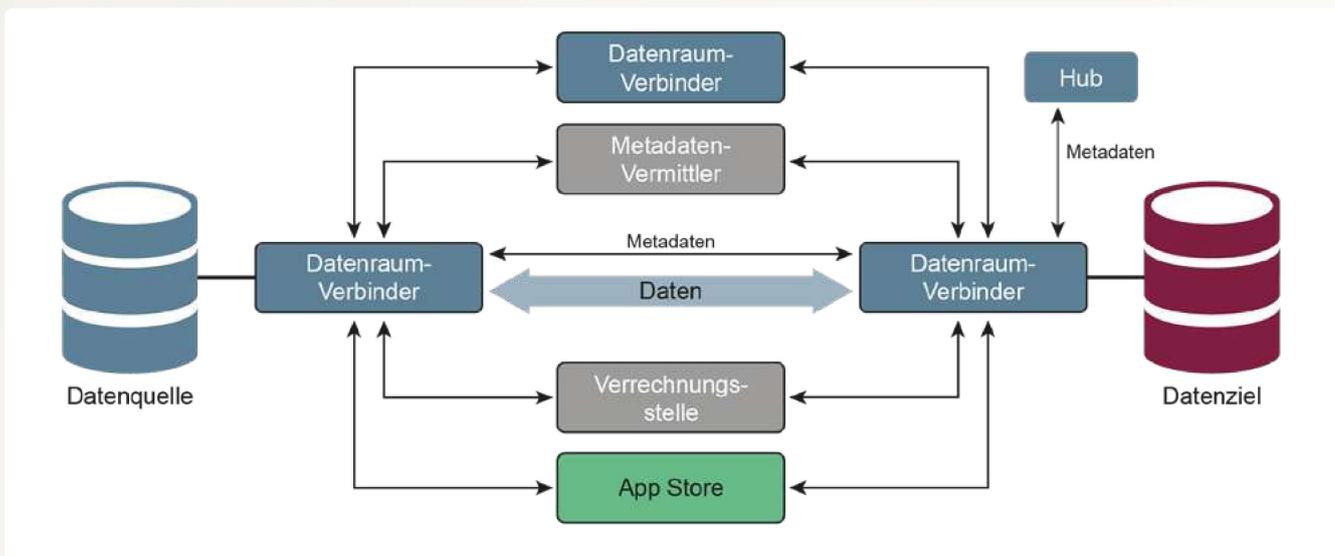
beschriebenen Systemkomponenten weitere Funktionen, die den Datenaustausch vereinfachen sollen. Dazu gehören unter anderem ein Berechtigungsmanagementsystem, OCR-Bilderkennung, Zertifizierungen und Wasserzeichen, Datenanalysetools und vieles mehr. Je nach Datenraum kann die Anzahl der Funktionen variieren<sup>[1]</sup>.

## EIGENSCHAFTEN

Gaia-X und die International Data Spaces Association (IDSA) veröffentlichen Publikationen, in denen die notwendigen Eigenschaften eines Datenraums definiert werden.

Es gibt Eigenschaften, die einen Datenraum ausmachen. So hat er notwendigerweise einen räumlichen und zeitlichen Umfang. Er sollte eine bestimmte Datenmenge und eine bestimmte Anzahl von Teilnehmenden über einen bestimmten Zeitraum umfassen. Ein Datenraum hat dezentral zu sein, es gibt also keine zentral gespeicherten Datensätze außerhalb des eigentlichen Kataloges. Um einerseits eine Dezentralisierung von Datenräumen zu ermöglichen und andererseits sicherzustellen, dass möglichst viele Teilnehmende miteinander in Austausch treten können, setzen die wichtigsten Datenrauminitiativen auf eine föderierte Struktur. Datenräume werden entsprechend interoperabel gestaltet und müssen notwendigerweise ein gewisses Maß an Transparenz aufweisen. Diese Transparenz bemisst sich an der Menge der Informationen, die über die Vorgänge im Datenraum, die tatsächlichen und potenziellen Beteiligten sowie betroffenen und nicht betroffenen Dritten zur Verfügung steht. Da ein Datenraum den Austausch von Daten voraussetzt, muss er ein gewisses Maß an Souveränität für die Teilnehmenden aufweisen.

Im Zusammenhang mit Transparenz und Souveränität steht der Begriff des Vertrauens<sup>[2]</sup>. Je mehr Transparenz besteht, sei es in Bezug auf die Datenqualität oder den Nachweis der Daten, und je größer die souveräne Kontrolle über die Daten ist, desto mehr können die Teilnehmenden dem Datenraum vertrauen. Die Vertrauenswürdigkeit von Datenräumen und deren Betreiber ist eine wesentliche Eigenschaft. Um eine Vertrauensbasis zwischen den Nutzern und dem Betreiber zu schaffen, sind Dienste nötig, die Zertifikate ausstellen und die Erfüllung von Vorschriften und Standards überprüfen. Die Befolgung der



Datenraum-Architektur/IDS-Architektur (Bild if(is))

Vorschriften spielt eine wichtige Rolle bei der Aufnahme neuer Teilnehmer und Dienste, da in einem Ökosystem wie einem Datenraum alle Parteien überprüfbar bleiben müssen. Zur Überprüfung werden Zertifikate an die Teilnehmer ausgegeben, die die Einhaltung der Richtlinien bescheinigen. Die Vertrauensbasis bildet die Grundlage für alle Datenräume, die auf einer bestimmten standardisierten Architektur basieren. Die Gaia-X-Plattform bietet zwei entscheidende Funktionen zur Sicherstellung der Compliance: das Gaia-X-Register, das einen Katalog konformer Dienste und Teilnehmer verwaltet, und die Compliance-API, die den Erwerb und die Authentifizierung von Zertifikaten überprüft [3].

Darüber hinaus kann der Nachweis nicht nur für Softwarekomponenten, sondern auch für Betriebsumgebungen erfolgen, beispielsweise für die Information-Delivery-Specification-(IDS)-Standards, die über das IDS-Zertifizierungssystem zertifiziert werden.

Bereits heute werden Datenräume in vielen Bereichen erfolgreich eingesetzt. In der Automobilindustrie, im Energiesektor ebenso wie im Gesundheitswesen oder im Rechtswesen. In den letzten Jahren sind in Europa branchenübergreifend neue Datenräume entstanden. Beispiele sind unter anderem der „Digital CSA“, der im Manufakturbereich oder auch bei erneuerbaren Energien aktiv ist. Im Mobilitätssektor ist der Vorreiter für Datenräume der Mobility Data Space. Im Gesundheitssektor sind im Jahr 2022 Datenräume entstanden, die bei der Bekämpfung von Krebs unterstützen sollen.

Die ersten Sektoren, die im Bereich Datenräume aktiv waren, sind das Energiewesen, die Land-

wirtschaft, Gesundheit, Finanzen, Mobilität und die Industrie mit der Initiative Industrie 4.0.

## DATENTREUHÄNDER

Ein Datentreuhänder ist eine vertrauenswürdige dritte Partei, die die Verantwortung für die sichere und ordnungsgemäße Verwaltung der Daten übernimmt, um die Interessen der Dateneigentümer zu schützen und die Einhaltung der geltenden Vorschriften zu gewährleisten. Die genaue Rolle und die Zuständigkeiten eines Datentreuhänders können je nach Kontext unterschiedlich sein.

Die Beziehung zwischen Datentreuhändern und Datenräumen besteht darin, dass Datentreuhänder maßgeblich an der Einrichtung und Verwaltung von Datenräumen beteiligt sind. Auch Behörden fungieren als Datentreuhänder, indem sie Daten, die als offene Daten bezeichnet werden, mit der Öffentlichkeit teilen. Dabei handelt es sich unter anderem um solche aus Bereichen wie Umwelt, Verkehr oder Energie, die auf Online-Portalen zur Verfügung gestellt werden. Ausgenommen sind personenbezogene Daten und andere sensible Informationen. Ein Beispiel aus der Praxis ist das Datenportal GoVData, das Verwaltungsdaten von Bund, Ländern und Kommunen öffentlich zugänglich macht. Unternehmen, die auf datengetriebenen Märkten tätig sind und eine marktbeherrschende Stellung innehaben, sollen künftig verpflichtet werden, einen Teil ihrer Daten zur Verfügung zu stellen. Welche Daten genau und mit wem geteilt werden müssen, ist noch nicht definiert. Von der Datenweitergabepflicht profitieren vor allem Unternehmen, die nicht über große Datenmengen verfügen, aber Daten für die Pro-

duktentwicklung benötigen. Beispiele für die Umsetzung einer allgemeinen und umfassenden Datenteilungspflicht sind allerdings noch nicht bekannt [4].

## REFERENZ-ARCHITEKTUREN

Der erste Referenz-Architekturansatz für den souveränen Datenaustausch wurde 2015 von der International Data Spaces Association (IDSA) entwickelt. IDSA hat derzeit über 100 Mitglieder und hat sich zum Ziel gesetzt, die Kontrolle an die Dateneigentümer zurückzugeben. Im IDS-Modell legen Dateneigentümer eigene Nutzungsrichtlinien für ihre Daten fest, etwa wer auf die Daten zugreifen darf und wie diese genutzt werden dürfen. Das International-Data-Space-Programm umfasst hauptsächlich drei Bereiche: Forschung, Standardisierung und Bereitstellung von Softwarediensten und -technologien für den Markt.

Auf der technischen Seite basiert die IDS-Architektur auf dem Konzept von Datenraum-Verbindern (Konnektoren) für jeden der Teilnehmer, die sowohl untereinander als auch in Datenräumen in Verbindung stehen. Der Datenraum-Verbinder fungiert als sicheres Gateway zwischen den Instanzen und ist für den Datenaustausch verantwortlich [5].

Die Prozesse innerhalb des Datenraum-Verbinders sind in zwei Bereiche unterteilt: die Steuerebene und die Datenebene. Die Kontrollschicht ist für alle Prozesse vor und nach der Transaktion verantwortlich: Identitäts- und Zugriffsverwaltung, Angebotsbearbeitung, Erstellung, Verhandlung und Abrechnung von Verträgen sowie

Protokollierung. Die einzige Aufgabe der Datenebene besteht darin, Daten nach erfolgreicher Vertragsverhandlung zu übertragen.

Dienste innerhalb des IDS sind modular und können somit kombiniert und erweitert werden. Dadurch ist es möglich, weitere Datenraum-Verbindungs-Implementierungen mit in den Datenraum einzubauen.

Die drei wichtigsten Datenraum-Lösungen, die zum Aufbau eines eigenen Datenraums verwendet werden, sind: Eclipse Dataspace Komponente (EDC), Gaia-X Federation Services (GXFS), Gaia-X Web3 Ecosystem (Web3) [1].

Der Eclipse Dataspace Konnektor und die zugehörigen Dataspace-Komponenten bieten ein modulares, erweiterbares Framework, das auf dem IDS-Framework basiert und gleichzeitig kompatibel zu Gaia-X ist. Die Gaia-X-Föderationsdienste stellen die technischen Mindestanforderungen und Dienste dar, die für den Betrieb föderierter Gaia-X-Ökosysteme aus Infrastruktur und Daten benötigt werden. GXFS wird vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) auf der Grundlage eines Beschlusses des Deutschen Bundestages gefördert. Einen etwas anderen Ansatz für die technische Umsetzung eines Gaia-X-Ökosystems verfolgt Pontus-X, das Gaia-X Web3-Ökosystem und GEN-X-Netzwerk der deltaDAO AG. Dieses Ökosystem basiert auf Web3-Technologien und nutzt eine Blockchain und Smart Contracts als sicheren, verteilten Speicher [1]. Tabelle 1 stellt die drei Systeme gegenüber.

Derzeit ist die Interoperabilität zwischen verschiedenen Referenzarchitekturen begrenzt möglich, besonders auf der Ebene der einzelnen Dienste und Komponenten. Allerdings gewährleisten gemeinsame Standards zur Beschreibung von Diensten und Architekturen ein gewisses Maß an Kompatibilität. Alle Datenraumlösungen verstehen die gleichen maschinenlesbaren Metadaten. Identifizierungs-Vertrauensanker können auch gemeinsam genutzt werden, sodass dieselben Anmeldeinformationen zur Identifizierung von Akteuren in verschiedenen Datenräumen verwendet werden können. Interoperabilität ist ein wichtiges Ziel für alle Organisationen, die an der Entwicklung einer verteilten Datenwirtschaft beteiligt sind [1].

Um Datenräume zu schaffen, ist es unerlässlich, die Offenheit und Zusammenarbeit zwischen

	EDC	GXFS	Web3
Identität und Vertrauen	IAM-Modul (oauth, daps)  Identity Hub	Authentifizierungs- und Autorisierungsdienste  Beglaubigungsmanager für Organisationen  Beglaubigungsmanager für Personen	DID im Gen-X-Chai SSI-Wallet
Katalog	Föderierter Katalog	Föderierter Katalog  Selbstbeschreibungstool	Föderierter Katalog: On Chain smart Contracts für Metadaten Cache für Metadaten  Aquarius: Cache für Metadaten
Austausch	Datenebene mit Erweiterungen für verschiedene Protokolle  Steuerungsebene für Vertragshandlung	Datenvertragsaktionsdienst  Datenaustauschprotokollierungsdienst	Datenvertragsdienst: Smart Contracts mit Datentoken  Datenaustausch-Protokollierungsdienst: Prüfpfad on chain  Compute to Data-Umgebung
Einhaltung der Vorschriften	Trust Framework Adoption  Policy Engine	Validierung als Teil der Authentifizierung/Autorisierung  Kontinuierlicher automatisierter Überwachungsdienst  Beglaubigungsdienst	Validierung als Teil einer SSI-Schicht
Andere	Datendashboard  Registration Service	Portal  Notarisierungsdienst	Portal

Tabelle 1: Gegenüberstellung Datenraumlösungen

den Teilnehmern zu optimieren. Die technische Umsetzung sollte an die spezifischen Bedürfnisse jedes Teilnehmers angepasst werden und gleichzeitig die vereinbarten Richtlinien und rechtlichen oder geschäftlichen Anforderungen der jeweiligen Branche oder des jeweiligen Bereichs einhalten.

Der Beitritt zu den Communities der entsprechenden Open-Source-Projekte ist nicht nur für die Entwickler von Vorteil, sondern auch für die Nutzer, um Unterstützung zu erhalten und die zukünftige Entwicklung mitzugestalten. Dies fördert die bestehende aktive Community sowie die technische Konvergenz für eine wirklich offene Datenwirtschaft.

Mit dem Data Governance Act hat die Europäische Kommission den Grundstein für die Schaffung eines europäischen Datenaustauschmodells gelegt. Das Hauptziel dieser Maßnahme ist es, Vertrauen in die gemeinsame Datennutzung zu schaffen, indem klare Vorschriften und Regeln festgelegt werden.

Ein Schlüsselement der Verordnung ist die Verpflichtung, die gesammelten Daten ausschließlich für die Zwecke der Datenvermittlung zu verwenden. Des Weiteren wurde festgelegt, dass die initialen Datenformate nicht verändert werden dürfen. Um die Einhaltung dieser Pflichten zu garantieren, sind Überwachungseinrichtungen notwendig, die sicherstellen, dass

die Diensteanbieter und Datenvermittler sich an die festgelegten Regeln halten. Dadurch wird gewährleistet, dass die gemeinsame Datennutzung reibungslos und unter klaren rechtlichen Rahmenbedingungen stattfindet, was das Vertrauen in den Datenaustausch fördert.

## HERAUSFORDERUNGEN FÜR KLEINE UND MITTLERE UNTERNEHMEN

Wenn auf Daten zugegriffen wird und diese weitergegeben werden, ohne dass die entsprechenden Schutzmechanismen zum Beispiel für personenbezogene Daten vorhanden sind, können Unternehmen wegen Nichteinhaltung der Datenschutzvorschriften mit Bußgeldern belegt werden.

Weiterhin ist es für viele kleine und mittlere Unternehmen (KMU) schwierig, sich in der Regulierungslandschaft zurechtzufinden und zu verstehen, welche Maßnahmen im Zusammenhang mit Daten zulässig sind. Ohne die Möglichkeit zu kontrollieren, wer und zu welchem Zweck die bereitgestellten Daten verwendet, sind die Folgen nicht absehbar. Werden Daten beispielsweise auf eine Art und Weise benutzt, die nicht den gesetzlichen Bestimmungen entspricht, kann das den Ruf des betreffenden Unternehmens schädigen oder eben Geldstrafen nach sich ziehen. Die Angst, die Kontrolle über die eigenen Daten zu verlieren, ist daher manchmal so groß, dass sich viele Unternehmen gegen Cloud-Computing entscheiden. Wenn KMU allerdings keine Cloud-Infrastruktur aufgebaut haben, können sie nicht wie andere Unternehmen von der gemeinsamen Nutzung von Daten profitieren.

Zudem werden die Rahmenbedingungen für den Zugang, die gemeinsame Nutzung und die Weiterverwendung von Daten meistens durch spezifische Einzelverträge geregelt. Das bietet den Beteiligten zwar die Flexibilität, spezifische Bedürfnisse zu berücksichtigen, führt aber

häufig zu dem Problem, dass sich KMU in einer schwächeren Verhandlungsposition befinden. Sie verfügen über weniger Ressourcen als größere Unternehmen, um faire Nutzungsbedingungen sicherzustellen.

Viele der genannten Gründe, die aus Sicht der KMU gegen einen Datenaustausch sprechen, sind auf mangelndes Vertrauen zurückzuführen. Um dieses Vertrauen herzustellen, muss ein Rahmen geschaffen werden, der es ihnen ermöglicht, rechtliche Probleme zu vermeiden, die Kontrolle über die bereitgestellten Daten zu behalten und diese nicht zu gefährden.

## WEITERENTWICKLUNG DER DATENRÄUME IN DEUTSCHLAND

Seit Anfang 2022 unterstützt und begleitet German Gaia-X elf Förderprojekte des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK). Im Fokus stehen praxisnahe Anwendungen von Datenräumen im digitalen Ökosystem für die Branchen Mobilität, Finanzen, Gesundheit, Bau, Geoinformation und Bildung.

Die entwickelten Anwendungsbeispiele sollen zeigen, wie Daten genutzt werden können, um Mehrwerte und neue, marktwirksame Geschäftsmodelle für KMU, Organisationen und Verwaltungen im Gaia-X-Ökosystem zu schaffen. Die erarbeiteten Best Practices und Lösungsansätze tragen dazu bei, die Entwicklung und Etablierung neuer datenbasierter Geschäftskonzepte in Deutschland und Europa zu inspirieren und praktisch zu unterstützen.

Das Förderprojekt Autowerkstatt 4.0 hat zum Beispiel das Ziel, eine sichere und vertrauenswürdige Plattform für den Austausch von Branchendaten und KI-Modellen zu schaffen, um die Digitalisierung der mittelständischen Fertigungsindustrie voranzutreiben und Fertigungsunternehmen und Messsystemanbieter über

Gaia-X in einem Innovations- und Wertschöpfungsnetzwerk zu verbinden.

Im Förderprojekt HEALTH-X dataLoft stehen die eigenen Gesundheitsdaten der Bürgerinnen und Bürger im Mittelpunkt. Ziel ist die Entwicklung transparenter cloudbasierter Anwendungen nach Gaia-X-Standards in hochrelevanten Bereichen der Gesundheitsversorgung wie Gesundheitsprävention, gesundes Altern und klinische Versorgung. Für die Vernetzung der Gesundheitsbereiche und die integrative Datennutzung werden Konzepte der Medizininformatik-Initiative sowie rechtsverbindliche Gematik-Standards und Lösungen der Telematikinfrastruktur integriert.

Darüber hinaus gibt es viele weitere zukunftsweisende Datenraumprojekte, die zeigen, welchen Stellenwert das Thema in Deutschland in bestimmten Bereichen derzeit bereits hat. Dennoch haben wir das Potenzial noch lange nicht ausgeschöpft <sup>[5]</sup>. ■



**JAN ROTTHUES**

studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Datenräumen.



**NORBERT POHLMANN**

ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrust und im Vorstand des Internetverbandes – eco.

### Literatur

<sup>[1]</sup> V. Siska, V. Karagiannis, M. Drobits, „Aufbau eines Datenraums: Technischer Überblick“, gaia-x Hub Austria, 2023, [www.gaia-x.at/wp-content/uploads/2023/04/WhitepaperGaiaX\\_german.pdf](http://www.gaia-x.at/wp-content/uploads/2023/04/WhitepaperGaiaX_german.pdf)

<sup>[2]</sup> N. Pohlmann, „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer-Vieweg Verlag, Wiesbaden 2022

<sup>[3]</sup> C. Niebel, A. Reiberg, P. Kraemer, White Paper: „Gaia-X für KMU“, gaia-x-hub.de, Februar 2022, <https://gaia-x-hub.de/white-paper-kmu/>

<sup>[4]</sup> Bundesministeriums für Wirtschaft und Klimaschutz, „Bundesministeriums für Wirtschaft und Klimaschutz.“, 2023, [www.iit-berlin.de/wp-content/uploads/2023/02/SDW\\_Datentreuhand.pdf](http://www.iit-berlin.de/wp-content/uploads/2023/02/SDW_Datentreuhand.pdf)

<sup>[5]</sup> International-Data-Spaces-Association. [github.com/International-Data-Spaces-Association/](https://github.com/International-Data-Spaces-Association/), 2023, [https://github.com/International-Data-Spaces-Association/IDS-RAM\\_4\\_0/tree/main/documentation/3\\_Layers\\_of\\_the\\_Reference\\_Architecture\\_Model/3\\_5\\_System\\_Layer](https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0/tree/main/documentation/3_Layers_of_the_Reference_Architecture_Model/3_5_System_Layer).

<sup>[6]</sup> gaia-x Hub Germany Fördervorhaben, <https://gaia-x-hub.de/gaia-x-foerdervorhaben/>