

WHITEPAPER

Aufbau eines Datenraums: Technischer Überblick

Kontakt:

Veronika Siska (veronika.siska@ait.ac.at)

Vasileios Karagiannis (vasileios.karagiannis@ait.ac.at)

Mario Drobics (mario.drobics@gaia-x.at)

1 Einführung

1.1 Motivation

In der heutigen digitalisierten Welt werden große Datenmengen generiert, aber wir können ihren Wert nicht in vollem Umfang nutzen. Die gemeinsame Nutzung von Daten könnte innovative datengesteuerte Anwendungen vorantreiben, bei der Erfüllung gesetzlicher Vorschriften helfen und einen finanziellen Wert schaffen. Organisationen zögern jedoch, ihre Daten miteinander zu teilen, weil sie befürchten, die Kontrolle darüber zu verlieren, wer auf sie zugreifen kann und wofür sie verwendet werden. Damit Daten routinemäßig zwischen Organisationen ausgetauscht werden können, ist eine kollaborative Umgebung, ein so genannter Datenraum, erforderlich, in dem die Teilnehmer:innen Daten und damit verbundene Dienste sicher austauschen und nutzen können und in dem etablierte technische und rechtliche Standards das Vertrauen gewährleisten.

Es gibt verschiedene Initiativen, die Software für Datenräume entwickeln, aber es fehlen Richtmaße zu den Fähigkeiten, dem Status und der Nutzbarkeit dieser verfügbaren Tools und zu der Implementierung von Datenräumen für bestimmte Zwecke. Das Ziel dieses Whitepapers ist es, die Lücke zwischen High-Level-Konzepten und rahmenspezifischer technischer Dokumentation zu schließen und einen Überblick über die aktuelle technische Landschaft der Datenraumkomponenten zu geben. Da der Fortschritt in vielen datenraumrelevanten Projekten rasant ist, soll dieses Dokument einen Leitfaden bieten, der dem:r Leser:in hilft, sich mit der gängigen Terminologie, dem aktuellen Stand der Technik und den vorhandenen Softwareanwendungen vertraut zu machen.

1.2 Datenraum

Ein Datenraum ist eine dezentralisierte, offene Infrastruktur für den souveränen Datenaustausch, deren Teilnehmer:innen sich der von ihnen produzierten und konsumierten Daten sowie der beteiligten Dienste (Hardware und Software) bewusst sind und diese kontrollieren.

Vor mehr als 15 Jahren tauchte das Konzept der Datenräume in der Informatik auf, welches eine Verlagerung von zentralen Datenbanken zur Speicherung von Daten an der Quelle vorsah [1]. Die Forschungen am Fraunhofer ISST führten diese Idee weiter und mündeten im Jahr 2015 schließlich in der Gründung der International Data Spaces Association [2] und der Erarbeitung eines ersten Konzepts und Standards für Datenräume. Deren Referenzarchitektur, das International Data Spaces Reference Architecture Model (IDS RAM) [3] beschreibt die notwendigen Komponenten und deren Anforderungen im Detail.

Gaia-X [4] ist eine europäische Initiative, die darauf abzielt, einen föderierten und sicheren Rahmen [5], [6] für den hoheitlichen Datenaustausch zu schaffen. Dabei geht Gaia-X noch einen Schritt weiter als das Datenraumkonzept, indem es generische datenbezogene Dienste wie Speicher und Webserver berücksichtigt, um die Interoperabilität zwischen verschiedenen Cloud-Anbietern und IT-Infrastrukturen zu ermöglichen.

Diese verschiedenen Initiativen haben noch diverse technische und nichttechnische Herausforderungen zu bewältigen. So gibt es zwar bereits die Software für den Datenaustausch, aber es fehlen noch die Verfahren und technischen Lösungen, die die Interoperabilität ermöglichen, die Einhaltung der Rechtsvorschriften gewährleisten und das Vertrauen in das Ökosystem stärken. Auch die Geschäfts- und Verwaltungsmodelle für den Betrieb und die Nutzung solcher Datenräume befinden sich noch in der Entwicklung. Der Schlüssel zu allen Bereichen ist die Zusammenarbeit, die durch Gemeinschaften und Initiativen erreicht wird, die Organisationen in Regierungen, Hochschulen und dem privaten Sektor umfassen. Viele der derzeit entwickelten Datenräume zielen darauf ab, eine föderierte, offene Infrastruktur für den hoheitlichen Datenaustausch auf der Grundlage gemeinsamer Standards und Regeln anzubieten.

1.3 Gaia-X

Das Projekt Gaia-X will einen Rahmen schaffen, in dem sich alle beteiligten Organisationen aus den verschiedenen Sektoren auf ein einheitliches Regelwerk einigen und so die Einhaltung wesentlicher Werte sicherstellen: Datenhoheit, Datenschutz, Vertraulichkeit, Sicherheit, Technologieneutralität und Interoperabilität. Ziel des Gaia-X-Projekts ist es, Organisationen, Unternehmen und Nutzer:innen die Möglichkeit zu geben, Daten effizient und kostengünstig zu verarbeiten und auszutauschen und gleichzeitig die Kontrolle über sie zu behalten - nicht nur darüber, wo diese Daten gespeichert werden, sondern auch darüber, wer sie für welche Zwecke nutzen darf. Gaia-X ist also weder ein neues europäisches Rechenzentrum noch ein neuer Cloud-Dienst.

Das Projekt Gaia-X wurde im Januar 2021 von 22 französischen und deutschen Unternehmen und Organisationen ins Leben gerufen und ist inzwischen zu einer europäischen Initiative geworden. Seine Organisation besteht aus drei grundlegenden Säulen: der Gaia-X European Association for Data and Cloud AISBL auf EU-Ebene, den nationalen Gaia-X Hubs in mehreren EU-Mitgliedstaaten und darüber hinaus, sowie der Gaia-X Community. Gaia-X wurde als gemeinnütziger Verein in Brüssel unter dem Namen Gaia-X Association internationale sans but lucratif (AISBL) gegründet und hat derzeit rund 370 Mitglieder (Stand 03/2023).

Um die Prinzipien und Werte von Gaia-X zu verwirklichen, wird derzeit das Gaia-X Framework [6] entwickelt, das geeignete Spezifikationen und Softwarekomponenten umfasst. Die Entwicklung des Gaia-X Frameworks erfolgt unter der Koordination der Gaia-X Association. Sie sollen es Organisationen ermöglichen, Daten und damit verbundene Dienste untereinander auszutauschen und gleichzeitig die Kontrolle über deren Nutzung zu behalten. Um ein vollständig transparentes Ökosystem zu schaffen, zielt Gaia-X auch darauf ab, das Daten- und das Infrastruktur-Ökosystem miteinander zu verbinden, d. h. die virtuellen Datenressourcen und die zugrunde liegenden Infrastrukturdienste wie Speicher-, Rechen- oder Netzlösungen. Beispiele für spezifische Dienste sind die Identifizierung der teilnehmenden Organisationen, die Darstellung der verfügbaren Datendienste, die automatische Überwachung der Einhaltung der Gaia-X-Regeln oder die notariellen Dienste für die Vorbereitung von Verträgen.

Gaia-X unterscheidet zwischen Föderationen und Datenräumen. Gaia-X-Föderationen sind selbstbestimmte Ökosysteme von Teilnehmer:innen, die Dienste konsumieren, produzieren, betreiben oder anbieten können, während ein Datenraum auch spezifische Dienste für den Datenaustausch wie Konnektoren oder die Durchsetzung von Nutzungsrichtlinien umfasst. In diesem Zusammenhang ist das Ziel einer Föderation die Verwaltung ihrer Teilnehmer:innen und Angebote, während sich Datenräume auf den Austausch von Daten in einem bestimmten Bereich konzentrieren.

Die Gaia-X Association publiziert alle Spezifikationen des Gaia-X Frameworks [6], [7] und stellt den Softwarecode für die Einhaltung dieser unter einer Open-Source-Lizenz öffentlich zur Verfügung für alle Interessierten wie zum Beispiel: Industrieunternehmen, KMUs, Start-ups, Forschungseinrichtungen, Organisationen der öffentlichen Verwaltung, Entwickler:innen, IT- und Cloud-Anbieter:innen. All diese Akteure können ihre Produkte und Dienstleistungen vorstellen, Daten austauschen und gemeinsam innovative Geschäftsmodelle auf der Grundlage der Gaia-X-Prinzipien und mit Hilfe des Gaia-X Frameworks entwickeln.

Das Projekt Gaia-X soll die Innovation in allen Wirtschaftsbereichen fördern und die zunehmende Abhängigkeit von einer Handvoll marktbeherrschender Unternehmen abmildern. Während Europa das Rennen um den Markt für Cloud-Infrastrukturen bereits verloren haben mag, werden die Karten für den Handel mit Daten gerade erst neu gemischt.

Gaia-X bietet einen Rahmen, der grundlegende europäische Prinzipien umfasst: Souveränität, Offenheit, Fairness, Sicherheit und Vertrauen. Es wird daher nicht nur einigen wenigen großen Akteuren dienen,

sondern unzähligen Unternehmen und Organisationen weltweit die Teilnahme am digitalen Markt erleichtern.

1.3.1 Gaia-X Framework

Das Gaia-X Framework [6] stützt sich auf 3 konzeptionellen Säulen: Regelkonformität, Föderation Services und Datenaustausch. Gaia-X-Regelkonformität-Dienste sind dezentrale Dienste, die das Vertrauen fördern, während Föderation-Dienste interoperable und übertragbare Dienste für das Ökosystem adressieren und Datenaustauschdienste für die eigentlichen Transaktionen einschließlich Vertragsabschluss, Zugangs- und Nutzungskontrolle und Protokollierung verantwortlich sind. Für jede dieser Säulen bietet Gaia-X funktionale und technische Spezifikationen sowie Open-Source-Softwarekomponenten für Regelkonformität-Dienste (siehe Links auf [6]). Darüber hinaus baut das Gaia-X-Framework auf dem Konzept der Gaia-X Digital Clearing Houses (GXDCH) auf, die als Ausführungsknotenpunkte für Regelkonforme-Dienste dienen.

1.4 Internationale Datenräume (IDS)

Die ersten Referenzarchitekturansätze für den hoheitlichen Datenaustausch wurden im Jahr 2015 von der International Data Spaces Association [2] gegründet. Die IDSA hat mittlerweile mehr als 100 Mitglieder:innen und hat sich zum Ziel gesetzt, die Kontrolle an die Dateneigentümer zurückzugeben. Im IDS-Modell legt der Dateneigentümer individuelle Nutzungsrichtlinien für seine Datenbestände fest, die z.B. definieren, wer auf die Daten zugreifen darf und wie sie genutzt werden können. Die Initiative International Data Spaces ist in drei Hauptbereichen tätig: Forschung, Standardisierung und Bereitstellung von Softwarediensten und Technologien für den Markt.

Die vier Hauptziele von IDSA sind die Vertrauensbildung, die Gewährleistung von Sicherheit und Datenhoheit, die Ermöglichung von Datenökosystemen und die Ermöglichung standardisierter Interoperabilität. Jede:r Teilnehmer:in sollte sowohl dem System als auch den anderen Teilnehmer:innen vertrauen und sicher sein, dass Daten nur unter gegenseitig vereinbarten Bedingungen und über vertrauenswürdige Kanäle ausgetauscht werden können. Bei IDS wird die Vertrauenswürdigkeit des Systems durch die Zertifizierung jedes:r Teilnehmer:in und jeder Softwarekomponente sichergestellt. Datensouveränität - d. h., dass die Teilnehmer:innen in Bezug auf ihre Daten völlig selbstbestimmt sind - ist die wesentliche Grundlage und das Hauptziel der gesamten IDS-Architektur. Die Datensouveränität kann neue Datenökosysteme mit eigenen kooperativen Geschäftsmodellen ermöglichen. Damit solche Datenökosysteme miteinander interagieren können, ist auch die Interoperabilität ein Teil des IDS. Daher bietet das IDSA ein umfassendes Datenraumprotokoll [8] das Nachrichten und API-Bindungen auf der Grundlage von DCAT und ODRL definiert.

1.4.1 IDS-Referenzarchitektur-Modell

Das IDS-Referenzarchitekturmodell [3] bietet Spezifikationen und Schemata für organisatorische Rollen und Verantwortlichkeiten sowie für technische Komponenten. Es unterscheidet vier verschiedene Geschäftsrollen: Teilnehmer:innen sind Nutzer:innen des Datenraums, die Daten bereitstellen und verbrauchen; Vermittler:innen oder "Plattformen" bieten vertrauenswürdige Dienste innerhalb des Datenraums an, z. B. die Speicherung und Verwaltung von Metadaten oder das Angebot von Analysediensten; Softwareentwickler:innen sind IT-Unternehmen, die den Teilnehmer:innen des Datenraums Software zur Verfügung stellen; und schließlich sind die Verwaltungsorgane für die Schaffung von Vertrauen und die Verbesserung der Interoperabilität verantwortlich, indem sie Zertifizierungen und Standards bereitstellen, durchsetzen und validieren.

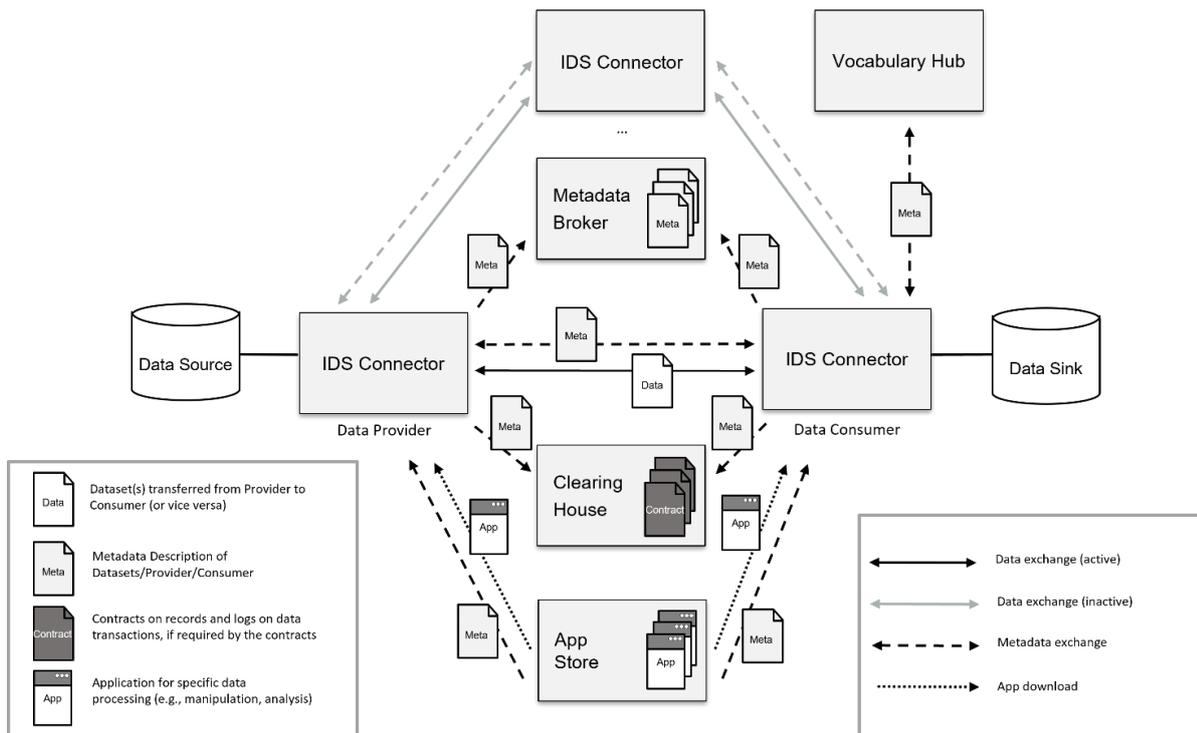


Abbildung 1: Systemdiagramm des IDS RAM, aus [Abschnitt 3.5: Systemschicht des IDS RAM 4.0.](#)

Auf der technischen Seite basiert die IDS-Architektur auf dem Konzept der Konnektoren für jede:n Teilnehmer:in, die sowohl untereinander als auch mit zusätzlichen, dem Datenraum gemeinsamen Diensten kommunizieren. Die Konnektoren fungieren als sichere Gateways zwischen den Einheiten und sind für den Datenaustausch untereinander zuständig. Die Prozesse innerhalb der Konnektoren sind in zwei Bereiche unterteilt: die Steuerungsebene und die Datenebene. Die Steuerungsebene ist für alle Prozesse im Vorfeld und im Anschluss an eine Transaktion zuständig: Identitäts- und Zugriffsmanagement, Bearbeitung von Angeboten, Erstellen, Aushandeln und Abrechnen von Verträgen sowie Protokollierung. Die einzige Aufgabe der Datenebene besteht darin, nach einer erfolgreichen Vertragsaushandlung (die von der Steuerungsebene beobachtet wird) Daten zu übertragen. Zu den Komponenten des IDS-RAM gehören neben den Konnektoren ein Identitätsanbieter für die Authentifizierung und Autorisierung, ein Metadaten-Broker für die Interaktion mit Metadaten im Katalog, ein Clearing House für die Protokollierung von Transaktionen und ein App Store für zusätzliche Datendienste.

Die Dienste im IDS-RAM sind modular aufgebaut und können somit kombiniert und erweitert werden. Dadurch ist es beispielsweise möglich, eine der IDS-Connector-Implementierungen mit einem Katalog oder einem Identitätsanbieter aus einem anderen Stack zu verbinden. In Anbetracht der vergleichsweise langen Geschichte von IDS gibt es bereits mehrere Implementierungen für Konnektoren und andere Dienste, sowohl unter Open-Source- als auch unter proprietären Lizenzen, die von allen möglichen Organisationen von der Wissenschaft über NROs bis hin zur Industrie genutzt werden.

Der Dataspace Konnektor [9] war der erste der Konnektoren und diente als Referenzimplementierung für seine Nachfolger. Er wurde ursprünglich am Fraunhofer ISST entwickelt und wird nun von der Sovity GmbH verwaltet [10]. Aufgrund der Kopplung zwischen der Kontroll- und der Datenebene, weist er einige Einschränkungen in Bezug auf den Datenaustausch auf. Es handelt sich jedoch um eine vollständige Implementierung mit allen Komponenten des IDS-RAM welches vor kurzem noch produktiv genutzt worden ist, z. B. vom Mobility Data Space [11] bis Ende März 2023. Der Eclipse Dataspace Konnektor mit seinen zugehörigen Dataspace Komponenten stellt den Nachfolger des ursprünglichen Dataspace Konnektors dar,

mit einer Architektur, die für Anwendungen auf Produktionsebene besser geeignet ist. Er wird ausführlich in Abschnitt 3.1 dieses Whitepapers beschrieben. Ein detaillierter Überblick über die verfügbaren Konnektoren ist im IDS Data Connector Report zu finden [12].

2 Dataspace-Architektur

Obwohl es verschiedene andere Initiativen im Zusammenhang mit Datenräumen gibt, werden wir uns auf Werkzeuge konzentrieren, die für Gaia-X-kompatible Datenräume entwickelt wurden, von denen einige mit IDS-kompatiblen Werkzeugen erstellt worden sind. Organisationen, die sich mit Datenräumen befassen, stellen Spezifikationen und Standards zur Verfügung, die befolgt werden können, sowie Referenzarchitekturen und Minimalimplementierungen. Letztere sind nicht als einzige Implementierung ihrer jeweiligen Rahmenwerke gedacht, sondern sollen vielmehr die Möglichkeiten aufzeigen und wiederverwendbare Softwarekomponenten und Werkzeuge bereitstellen. Es gibt nicht die eine beste Lösung für die Einrichtung eines Datenraums, aber die Einhaltung gemeinsamer Standards ist notwendig, um Interoperabilität zu ermöglichen. In diesem Abschnitt werden wir bestimmte technische Komponenten auf hoher Ebene erörtern, die in allen Datenräumen gleich sind. Durch die Etablierung einer gemeinsamen Sprache können wir uns bei der Beschreibung der verschiedenen Komponenten von Datenräumen auf diese Grundlagen beziehen. Im Allgemeinen kann eine Datenraumlösung aus verschiedenen Elementen (Systemkomponenten und Teilnehmer:innen) bestehen, von denen die wichtigsten in folgender Abbildung 2 dargestellt sind und in den folgenden Unterabschnitten näher erläutert werden:

- **Datenraum:** Aus der Systemperspektive ist ein Datenraum die Sammlung der notwendigen Komponenten, die den souveränen Austausch von Daten und Diensten ermöglichen. Wie in der Abbildung 2 dargestellt, können mehrere Datenräume im Rahmen desselben Regelkonformen-Dienstes nebeneinander bestehen.
- **Asset-Anbieter:** Eine Person oder Organisation, die einen Vermögenswert (z. B. einen Datensatz, einen Dienst usw.) anbietet, den sie besitzt/betreibt.
- **Asset-Konsument:** Eine Person oder Organisation, die einen Vermögenswert (z. B. einen Datensatz, eine Dienstleistung usw.) erwerben/verwenden möchte.
- **Konformitätsdienste:** Dienste, die alle anderen Komponenten des Systems validieren und die Interoperabilität sicherstellen.
- **Identitätsdienste:** Dienste, die glaubwürdige Identitäten bereitstellen und verwalten und das Vertrauen zwischen den Teilnehmer:innen des Systems ermöglichen.
- **Katalog:** Ein Verzeichnis von Vermögenswerten, das es Anbieter:innen ermöglicht, ihre Vermögenswerte zu veröffentlichen, und Verbraucher:innen nach verfügbaren Angeboten zu suchen.
- **Datenaustausch:** Dienste, die die Transaktion zwischen Anbieter:innen und Verbraucher:innen abwickeln, einschließlich Vertragsabschluss, Protokollierung und Datenübertragung.

2.2 Datenaustausch

Werkzeuge für den Austausch von Daten oder anderen Diensten sind ein wesentlicher Bestandteil eines Datenraums. Dazu können **Datenübertragung**, **Vertragsabschlüsse** zwischen Teilnehmer:innen, Festlegung und Durchsetzung von **Nutzungsrichtlinien**, **Protokollierung** von Transaktionen, **Audits usw.** gehören. Nicht alle diese Dienste sind obligatorisch; die Anforderungen hängen von der jeweiligen Art der Transaktion ab. Im einfachsten Fall kann eine Transaktion lediglich darin bestehen, bestimmten Bedingungen zuzustimmen und dann einen Link zum Herunterladen von Daten zu erhalten. Andererseits kann ein Datenraum auch etwas so Komplexes wie das Ausrollen von Diensten auf ein Kubernetes-Cluster und die anschließende

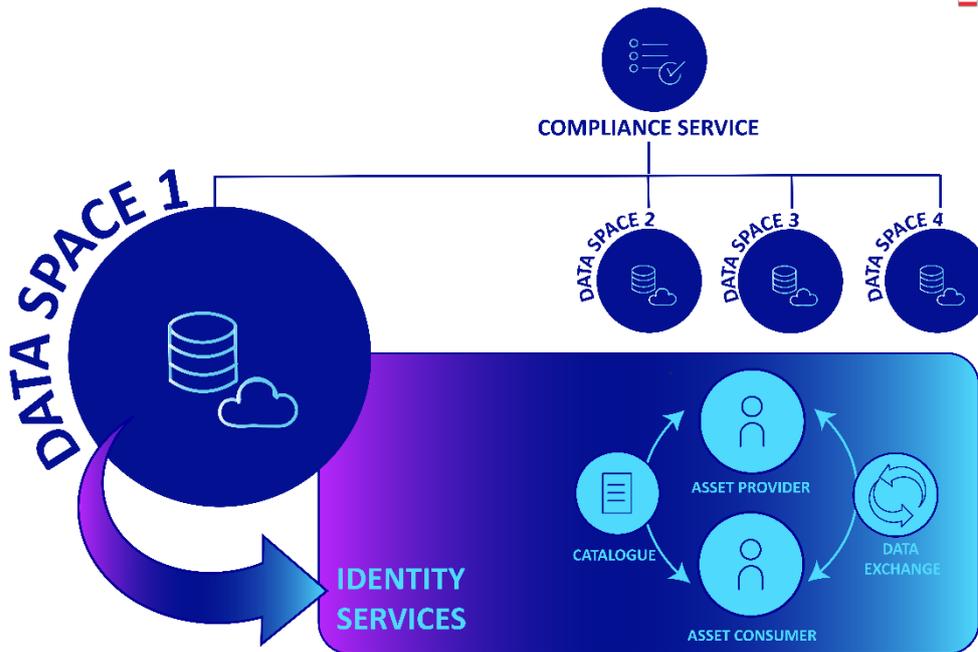


Abbildung 2 Grundelemente Gaia-X-kompatibler Datenräume (eigene Visualisierung des AIT)

Überwachung und Verwaltung dieser Dienste verwalten. Die Komplexität und die Art der technischen Hilfsmittel sollten an die Bedürfnisse des Datenraums angepasst werden und immer standardisierte, maschinenlesbare Beschreibungen verwenden, um Interoperabilität zu gewährleisten.

2.3 Katalog

Ebenfalls erforderlich ist ein **gemeinsamer Katalog**, der standardisierte Beschreibungen der Angebote enthält und den Teilnehmer:innen die Suche und Auswahl von Diensten ermöglicht. Diese Beschreibungen, die im Kontext von Gaia-X als Selbstbeschreibungen oder Metadaten bezeichnet werden, sollten erweiterbar (um den Bedürfnissen bestimmter Branchen gerecht zu werden) und überprüfbar (um Vertrauen zu schaffen) sein. Neben dem gemeinsamen Katalog von Metadaten kann ein Datenraum auch Dienste zur **Erstellung, Signierung und Verwaltung standardisierter Metadaten** anbieten. Die Anbieter:innen müssen in der Lage sein Dienste anzubieten und die Sichtbarkeit derer zu kontrollieren und die Verbraucher:innen müssen in der Lage sein, die für sie interessanten Dienste zu suchen und auszuwählen. Durch die Verwendung standardisierter Metadaten können solche Kataloge sogar ein verknüpftes und/oder verschachteltes Netz bilden. Die Vision von Gaia-X ist es, alle Angebote in einem gemeinsamen, synchronisierten Register zu sammeln und gleichzeitig zusätzliche Aggregatoren auf niedrigeren Ebenen zuzulassen (zentrale Datenbanken oder dezentralisierte Speicherung, z. B. auf verteilten Ledgern oder einfachem Webspeicher) sowie Sichtbarkeitsbeschränkungen, um kontrollierte oder private Datenräume zu ermöglichen.

2.4 Identität

Die nächste Kategorie von Diensten bezieht sich auf die Identitäten der Teilnehmer:innen um sie sicher identifizieren und ihre Rechte festlegen zu können, müssen sie **authentifiziert und autorisiert werden**. Diese Dienste umfassen die Bereitstellung, Verwaltung und Validierung von Identitäten auf der Grundlage eines zugrunde liegenden Vertrauensrahmens sowie von datenraumspezifischen Registern. Um den Teilnehmer:innen die Kontrolle über ihre eigenen Identitäten zu geben und dezentralisierte Identitäten für Dienste und Güter zu ermöglichen, bauen Datenräume häufig auf selbstverwalteten Identitäten (SSI) auf, obwohl auch ein föderierter Ansatz oder ein zentraler Identitätsanbieter möglich ist.

SSI kann mit Verifiable Credentials implementiert werden, wie es in einem W3C-Standard formuliert ist[13], dies ist eine Form von digitalen Zertifikaten, die kryptographisch signierte und damit fälschungssichere und automatisch überprüfbare Aussagen enthalten. In einem Datenraum können solche Berechtigungsnachweise verwendet werden, um vertrauenswürdige Aussagen über die Identität und Eigenschaften von

Teilnehmer:innen, Diensten und Angeboten zu machen. Es ist wichtig, dass sich die Teilnehmer:innen auf eine Reihe von Aussteller:innen einigen, denen sie vertrauen und deren Zertifikate sie alle akzeptieren. Für SSI sind zusätzliche Komponenten, so genannte **Wallets**, erforderlich, um Berechtigungsnachweise zu verwalten (anzufordern, zu speichern und zu präsentieren).

2.5 Regelkonformität

Um die Vertrauensbasis in Datenräumen zu schaffen, sind spezielle Dienste erforderlich, die **Zertifikate ausstellen und überprüfen**, um die Einhaltung von Vorschriften und Normen zu gewährleisten. Die Einhaltung der Vorschriften spielt eine Rolle bei der Aufnahme von Teilnehmer:innen und Diensten in ein Ökosystem und muss jederzeit überprüfbar bleiben. Diese Vertrauensschicht bildet die Grundlage für alle Datenräume, die auf einem bestimmten Rahmen basieren (z. B. Gaia-X). Datenräume können ebenfalls auch zusätzliche Regeln und Prüfungen hinzufügen.

Im Gaia-X Trust Framework [7] können Zertifikate, die die Compliance jeder Einheit signalisieren (Teilnehmer:innen, Ressource, Dienstangebot) in Form von Verifiable Credentials verliehen werden. Diese Konformitätszertifikate sind obligatorisch, um Teil des Gaia-X-Ökosystems zu sein, und zusätzliche Gütesiegel, die die Einhaltung spezifischer Regeln (z. B. Europäische Kontrolle, Art. 6 GDPR) bescheinigen, sind für geprüfte und überprüfte Dienstangebote erhältlich. Gaia-X bietet zwei Hauptkomponenten für die Regelkonformität: das Gaia-X-Registry mit konformen Diensten und Teilnehmer:innen und die Compliance-API, über die Zertifikate bezogen und überprüft werden können. Darüber hinaus können auf Datenraumebene sowohl Softwarekomponenten als auch Betriebsumgebungen zertifiziert werden, z. B. für die IDS-Standards unter Verwendung des IDS-Zertifizierungsschemas [14], [15].

Es ist wichtig zu beachten, dass die Dienste für die Einhaltung eines bestimmten Rahmens (z. B. Gaia-X) von dem jeweiligen Rahmen bereitgestellt (aber nicht notwendigerweise von ihm betrieben) werden müssen, während die Datenräume solche Dienste nutzen müssen, um selbst konform zu sein. Speziell für Gaia-X werden im neuesten Gaia-X Trust Framework die Gaia-X Digital Clearing Houses (GXDCH) als die Orte dienen, an denen die Konformität erreicht wird, wobei unabhängige Instanzen separat betrieben werden. Die Datenraumkomponenten, die die Einhaltung der Vorschriften ermöglichen, indem sie sich mit den Regelkonformität-Diensten (insbesondere mit denen von Gaia-X) verbinden, werden daher Teil unserer technologiestapelspezifischen Diskussion sein, nicht aber die Regelkonformität-Dienste selbst.

2.6 Zusätzliche Komponenten

Ein Datenraum kann weitere Komponenten enthalten, um die Nutzung zu erleichtern und bereichsspezifische Zusatzfunktionen bereitzustellen. Ein **Portal** ist für den benutzerfreundlichen Zugang zum Datenraum, einschließlich des Zugangs zu den Konten der Teilnehmer:innen und der Bereitstellung und Inanspruchnahme von Diensten, unerlässlich. Auch die **Orchestrierung** der bestellten Dienste oder Datenverarbeitungsanwendungen können die Kernfunktionalitäten ergänzen; sie können auf die Bedürfnisse der Teilnehmer:innen und die Arten des Austauschs im System zugeschnitten werden. Andere Plugins können zur **Durchsetzung von Regeln**, wie z. B. Nutzungsrichtlinien oder gesetzlichen Vorschriften, verwendet werden.

3 Datenraum-Stack

Im folgenden Abschnitt werden die drei wichtigsten Stapel vorgestellt, die zum Aufbau eines Datenraums verwendet werden können: die Eclipse Dataspace Komponente, die Gaia-X Federation Services und das Gaia-X Web3 Ecosystem. Für einen Überblick siehe

Tabelle 1. Wir werden uns auf die verfügbaren Dataspace-Komponenten in den jeweiligen Stapeln und die ihnen zugrunde liegende Technologie sowie auf die praktischen Auswirkungen (Vorteile und Einschränkungen) konzentrieren.

	EDC	GXFS	Pontus-X
Technologie	Modular aufgebaute Komponenten mit Java und Gradle	Modulare Komponenten, die hauptsächlich mit TypeScript erstellt werden	Blockchain-basierte Technologie auf dem Ocean Marketplace
Website	https://projects.eclipse.org/projects/technology.edc	https://www.gxfs.eu	https://portal.minimal-gaia-x.eu
Repository	https://github.com/eclipse-edc	https://gitlab.com/gaia-x/data-infrastructure-federation-services	https://github.com/deltaDAO/mvg-portal
Beispielhafte Projekte	Catena-X , Eona-X , Health-Xdata-Loft usw.	Geplante Übernahme durch deutsche Gaia-X-geförderte Projekte	EuProGigant , moveID , Staatsbibliothek zu Berlin , etc.

Tabelle 1: Grundlegende Fakten für die in diesem Whitepaper beschriebenen Datenraum-Stacks: die Eclipse Dataspace Components (EDC), die Gaia-X Federation Services (GXFS) und das Pontus-X Gaia-X Web3 Ecosystem & GEN-X Network (Pontus-X). Hinweis: Die Projektlisten sind nicht erschöpfend.

3.1 Eclipse Dataspace-Komponenten

Der Eclipse Dataspace Konnektor [16] und die zugehörigen Dataspace-Komponenten bieten ein modulares, erweiterbares Framework, das auf dem IDS-Framework basiert und gleichzeitig Gaia-X-Kompatibilität bietet. Im Gegensatz zu seinem Vorgänger, dem Dataspace Konnektor, sind beim Eclipse Dataspace Konnektor die Kontroll- und Datenebene getrennt und bieten somit eine bessere Skalierbarkeit. Die getrennte Verarbeitung des Datentransfers eignet sich besser für den Umgang mit großen Datenmengen oder komplexen Protokollen sowie für die Wiederverwendung bereits vorhandener Technologien innerhalb von Organisationsinfrastrukturen.

Das Projekt wird von der Eclipse Foundation gehostet und von einer Reihe von Datenräumen wie dem Gaia-X-Leuchtturmprojekt Catena-X [17] und Eona-X [18] verwendet. Es ist kompatibel mit dem IDS RAM, wird aber auch aktiv weiterentwickelt, um mit den Gaia-X-Standards konform zu sein, insbesondere mit dem Gaia-X Trust Framework [19]. EDC-Komponenten sind in Java geschrieben und mit Gradle erstellt, können aber in jede Art von Anwendung eingebettet werden. Das EDC-Projekt umfasst auch ein separates Repository für die Einrichtung eines Minimal Viable Dataspace (MVD) mit EDC-Komponenten, um die technische Einführung und das Onboarding zu unterstützen. Ein Überblick über die Architektur ist in Abbildung 4.

Der Konnektor kann Identitäts- und Zugriffsverwaltungsmodule (IAM) in drei Varianten verarbeiten: für das OAuth-Protokoll, für dezentrale Identitäten (DID) und für den Dynamic Attribute Provisioning Service (DAPS) von IDS. Für die Verwaltung von Identitäten für eine einzelne Entität (z. B. für die Bereitstellung von Zertifikaten im Falle von DID) ist auch ein Identitäts-Hub als separate Komponente verfügbar, die in der Konnektor-Umgebung ausgeführt werden kann. EDC bietet als Teil des Konnektors auch Katalogdienste an, die sowohl Datensätze der eigenen Datenbestände speichern als auch externe Daten crawlen und cachen können. Darüber hinaus gibt es einen separaten Dienst für die Verwaltung der Datenraum-Mitgliedschaft, den Registration Service, sowie eine Trust Framework Adoption-Schicht, die die Konfiguration des Gaia-X Trust Frameworks und der entsprechenden Richtlinien ermöglicht.

Die Datenebene ist als Modul des Konnektors implementiert, kann (und sollte in einer produktiven Umgebung) jedoch in einer separaten Umgebung ausgeführt werden. Es gibt Erweiterungen für verschiedene Protokolle, Datenquellen und Übertragungsmechanismen. Dazu gehören derzeit die Dateiübertragung über HTTP sowie Verbindungen zu den drei großen Blob-Storage-Diensten der Cloud-Anbieter: AWS, Azure und Google Cloud. Wie bei allen EDC-Diensten besteht die Möglichkeit, benutzerdefinierte Erweiterungen zu schreiben, die auf die Bedürfnisse bestimmter Datenräume zugeschnitten sind.

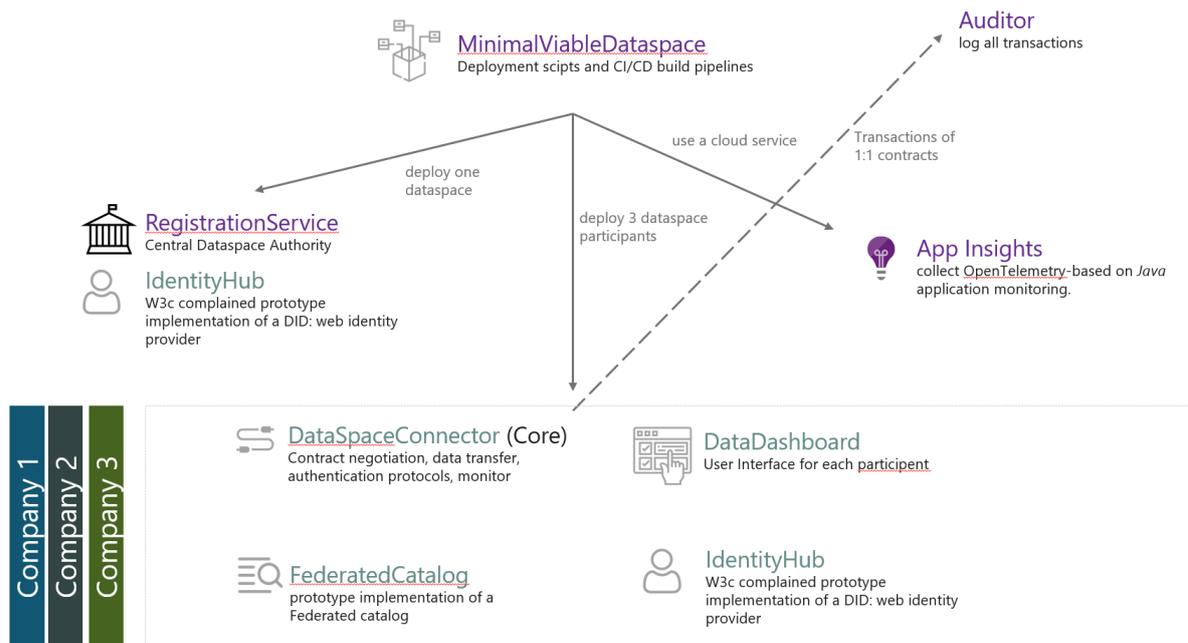


Abbildung 3: Architektur der Eclipse Dataspace-Komponenten am Beispiel des Minimal Viable Dataspace. Die Grafik wurde von den EDC-Maintainern zur Verfügung gestellt.3

3.2 Gaia-X Föderationsdienste

Die Gaia-X Föderationsdienste (GXFS)[20] 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. Das Projekt wurde ins Leben gerufen, um die Entwicklung von Gaia-X Föderation Services anzustoßen, die in einem gemeinsamen Community-Prozess spezifiziert wurden. Der eco - Verband der Internetwirtschaft e.V. mit Sitz in Köln koordiniert die Spezifikationsarbeiten und vergibt die Aufträge für die Umsetzung im Rahmen einer offenen EU-weiten Ausschreibung. Die Repositorien werden derzeit von der Gaia-X Association verwaltet und sollen an die Eclipse Foundation im Jahr 2023 übergeben werden.

GXFS basieren auf der Gaia-X-Architektur in der Version 21.03., Anpassungen an das neue Trust Framework in Version 22.04. sind jedoch in Arbeit. GXFS bietet sowohl Spezifikationen als auch Open-Source-Basiscode für das Minimum an Diensten, die für den Betrieb von Gaia-X Föderationsdienste erforderlich sind (siehe Abbildung 5). Solche Ökosysteme bestehen aus miteinander verbundenen Daten- und Infrastruktur-Ökosystemen, die in sogenannten Föderationen zusammengefasst sind und mit Hilfe von Föderationsdienste individuell orchestriert und betrieben werden. Es dient als Referenzimplementierung, aber auch andere Implementierungen sind möglich. GXFS umfasst nur die für den Betrieb einer Föderation notwendigen Dienste mit einem generischen Umfang: Sie berücksichtigen nicht nur den Datenaustausch, sondern auch andere Arten von Angeboten wie Cloud-Dienste, physische Maschinen oder Algorithmen. Die Durchführung des Datenaustauschs, zum Beispiel über Konnektoren, liegt jedoch außerhalb des Anwendungsbereichs. Die

Dienste von GXFS bilden eine modulare Toolbox, aus der Föderationen das auswählen und nutzen können, was sie benötigen, und Elemente nach Bedarf anpassen können.

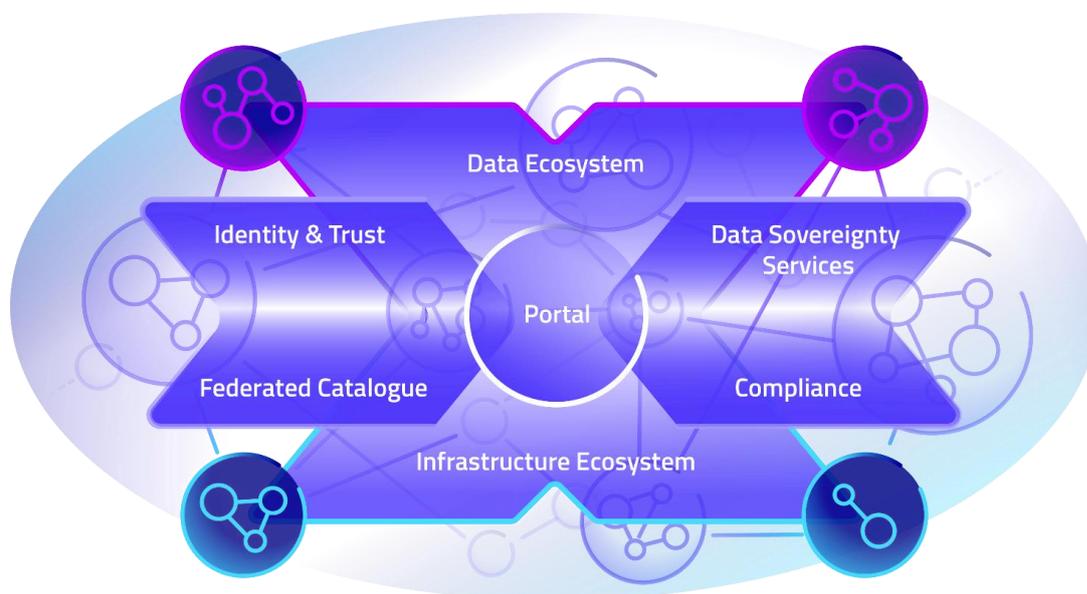


Abbildung 4: GXFS-Infrastrukturkomponenten aus den Arbeitsgruppen "Identität und Vertrauen", "Föderierter Katalog", "Portal", "Souveräner Datenaustausch" und "Regelkonformität", die das Infrastruktur- und Datenökosystem miteinander verbinden. Grafik zur Verfügung gestellt von eco - Verband der Internetwirtschaft.

Um transparente und vertrauenswürdige Transaktionen zu gewährleisten, bieten GXFS Datensouveränitätsdienste an - einen Datenvertragsdienst zur Erstellung und Verwaltung von Verträgen und einen Datenaustauschprotokollierungsdienst zur Verfolgung von Transaktionen und Ermöglichung von Prüfpfaden für die Vertragsparteien. Der Föderierter Katalog ist ein durchsuchbarer, aktueller Katalog von Metadaten (Selbstbeschreibungen), die innerhalb einer Föderation gemeinsam genutzt werden, und GXFS bietet auch zusätzliche Tools zur Erstellung, Visualisierung und Validierung solcher Selbstbeschreibungen für Teilnehmer:innen und Assets.

Die Identitäten in GXFS werden von den Authentifizierungs- und Autorisierungsdiensten verwaltet, die auch die Verwaltung dezentraler Identitäten und die Validierung von Teilnehmer:innen während des Onboarding-Prozesses umfassen. Außerdem werden getrennte Beglaubigungsmanager für Organisationen und natürliche Personen sowie Vertrauensdienste bereitgestellt, um das Vertrauen in Teilnehmer:innen und Dienste durch kryptografische Nachweise zu gewährleisten. Mit diesen Identitätsdiensten sind Compliance-Dienste verbunden: ein kontinuierlicher automatisierter Überwachungsdienst zur Überwachung der Konformität von Selbstbeschreibungen im föderierten Katalog und eine Notarisierungsdienst zur Erstellung überprüfbarer Darstellungen auf der Grundlage von Selbstbeschreibungen von Vermögenswerten und Teilnehmern.

GXFS bietet auch zusätzliche Dienste zur Unterstützung der Teilnehmer: ein Portal mit einer Benutzeroberfläche zur Integration aller Dienste und einen Orchestrierungsdienst zur Instanziierung und Verwaltung von Infrastrukturdiensten wie virtuellen Maschinen aus den Suchergebnissen des Föderierter Katalogs über das Portal.

3.3 Pontus-X

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. Die Komponenten bauen auf dem Ocean Protocol und dem Software-Stack von Polygon Labs auf, um die für Datenräume erforderlichen Föderationsdienste bereitzustellen [21] (für die Architektur, siehe Abbildung). Der Stack wird von Gaia-X-Leuchtturmprojekten, z.B. EuProGigant [22] und moveID [23] und anderen europäischen Initiativen verwendet. Alle Komponenten werden als Open-Source-Software unter einer Apache-2.0-Lizenz bereitgestellt.

Modular components, based on a DLT core grid, without lock-in

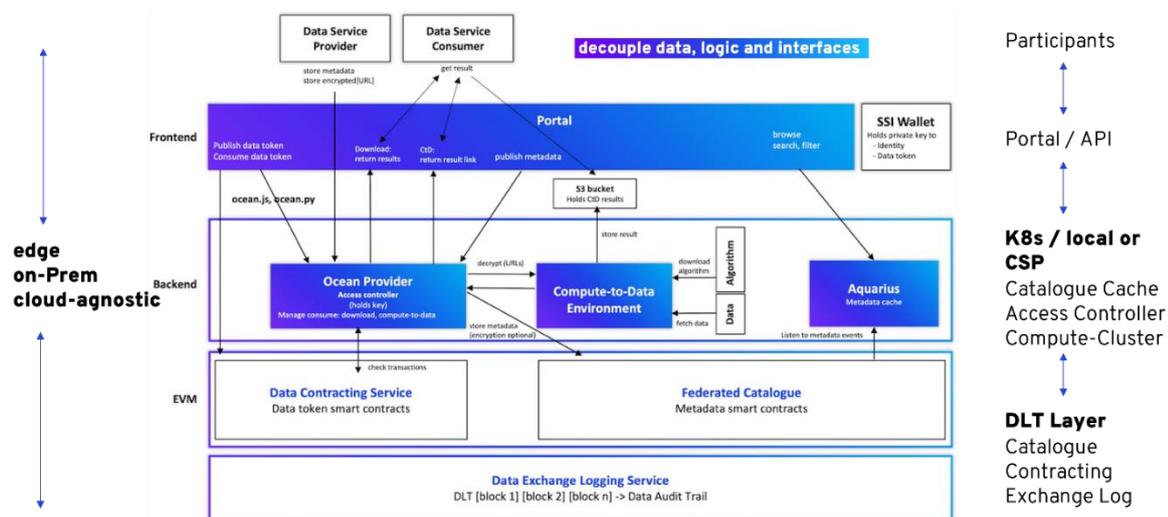


Abbildung 5: Beispielarchitektur für einen Service Provider im Gaia-X Web3 Ökosystem. Grafik zur Verfügung gestellt von deltaDAO AG.

Die aktuelle Implementierung verwendet eine eigene Ethereum Virtual Machine (EVM)-kompatible Blockchain, das GEN-X-Chain [24], das mit dem Polygon-Edge-Framework aufgebaut wurde und in Polygon-Supernets überführt werden soll. Um die Ausfallsicherheit des Netzwerks zu erhöhen, ist es sowohl geografisch als auch über europäische Cloud-Service-Provider verteilt; kann inzwischen jeder der zugrunde liegenden Dienste von einzelnen Service-Providern betrieben werden. Die GEN-X-Chain verwendet Proof of Authority (PoA), einen umweltfreundlichen und skalierbaren Konsensmechanismus, bei dem zugelassene Konten ("Validatoren") Transaktionen verifizieren und Blöcke erstellen dürfen. Das Netzwerk ist öffentlich zugelassen, was bedeutet, dass von der Gemeinschaft genehmigte und identifizierte Föderatoren beitreten können. Derzeit gibt es elf Validierer, die alle in Europa ansässig sind: Arsys (Spanien), BigchainDB (Deutschland), deltaDAO AG (Deutschland), EuProGigant (Österreich/Deutschland), Exoscale (Schweiz/Österreich/Deutschland), Ionos (Deutschland), Staatsbibliothek zu Berlin (Deutschland), Wobcom (Deutschland), Software AG (Deutschland), TU Wien (Österreich) und Universität de Lleida (Spanien), und weitere werden folgen. Die gemeinsame Blockchain dient auch als Interoperabilitätsschicht zwischen Datenräumen und Teilnehmern des Gaia-X Web3-Ökosystems: Sie können als Teilmengen von Teilnehmer:innen und Angeboten mit ihren eigenen Portalen, Infrastrukturen, angeschlossenen Netzwerken und optionalen zusätzlichen Regeln betrachtet werden. Der Katalog kann on-chain oder off-chain in Form von (optional verschlüsselten) Metadaten für jedes Serviceangebot gespeichert werden, auf die das Portal über einen Cache (Aquarius) oder direkt über das Netzwerk zugreift. Der Katalog kann entweder die vollständigen Metadaten und Gaia-X-konformen Selbstbeschreibungen in einzelnen ERC721-Smart Contracts oder als Zeiger auf einen Webservice oder dezentralen Off-Chain-Speicher speichern.

Verträge, die die Nutzungsbedingungen für Vermögenswerte festlegen, werden auf der Kette als Smart Contracts und als Teil der Selbstbeschreibungen des Dienstangebots aufgezeichnet, die wiederum off-chain oder on-chain gespeichert werden können. Smart Contracts werden automatisch ausgeführt, wenn Verbraucher und Dienstanbieter eine Vereinbarung unterzeichnen und die Bedingungen erfüllt sind. Nutzungsbeschränkungen (z. B. Download oder ausschließliche Nutzung für Berechnungen, Vertragsablauf, Lizenzierung, Zugangskontrolle und Preisgestaltung) können Teil dieser Verträge sein. Audit Trails werden durch die Protokollierung aller Transaktionen in der Blockchain ermöglicht. Dienste für SSI-basierte Authentifizierung und Autorisierung sind ebenfalls enthalten, wie z. B. rollenbasierte Zugriffskontrollen (RBAC) und fein abgestufte Berechtigungen. Eine vollwertige SSI-Integration einschließlich der Verarbeitung von REGO-Richtlinien durch SSI-Prüfer befindet sich derzeit in der Entwicklung. Darüber hinaus verlangt das Pontus-X-Ökosystem von allen Teilnehmern die Einhaltung des Gaia-X Trust Framework, indem sie Gaia-X-konforme Selbstbeschreibungen bereitstellen, die über den Gaia-X-Compliance-Service verifiziert werden.

Der zugrundeliegende Rahmen, Ocean Protocol, unterstützt den statischen und dynamischen Datenzugriff sowie die Durchführung von Berechnungen auf Daten, ohne direkt auf diese zuzugreifen, sondern nur die Ergebnisse zu erhalten ("compute-to-data"). Letzteres ebnet den Weg für die Wahrung und Verbesserung des Datenschutzes, die bedarfsorientierte Aggregation/Anonymisierung sowie die föderierte Analyse und das Lernen. Monetarisierung und sofortige Abrechnung sind ein wesentlicher Bestandteil des Stacks: Der Zugang zu einem bestimmten Angebot wird über einen eigenen ERC20-Utility-Token ("Daten-Token") verwaltet. Diese Daten-Token können derzeit im Austausch gegen anderen ERC20-Token (z. B. OCEAN-Token, EURO-Token) oder in Zukunft durch Off-Chain-Zahlungen, z. B. per Kreditkarte oder SEPA, erworben werden.

3.4 Zusammenfassung

Jeder der skizzierten Stacks kann zur Einrichtung eines Datenraums verwendet werden, auch durch eine Mischung dieser fertigen Komponenten aus den oben beschriebenen Stacks und kundenspezifischer Zusatzsoftware. Eine Zusammenfassung der verfügbaren Komponenten für jeden Stack ist in Tabelle 2 dargestellt.

	EDC	GXFS	Web3
Identität und Vertrauen	IAM-Module (oauth, did, daps)	Authentifizierungs- und Autorisierungsdienste	DID im GEN-X-Chain
	Identity Hub	Beglaubigungsmanager für Personen Beglaubigungsmanager für Organisationen	SSI-Wallet
Katalog	Föderierter Katalog	Föderierter Katalog Selbstbeschreibungs-Tools	Föderierter Katalog: On-chain smart Contracts 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	Daten-Dashboard (nur zur Demonstration)	Portal	Portal
	Registration Service	Notarisierungsdienst	

Tabelle 2: Hauptkomponenten für jedes Technologiepaket. Unter "Compliance" sind nur datenraumspezifische Dienste aufgeführt, nicht die vom Rahmenwerk bereitgestellten (z. B. Gaia-X).

4 Interoperabilität

Derzeit ist die Interoperabilität zwischen verschiedenen Ökosystemen/Stapeln begrenzt, insbesondere auf der Ebene der Softwarekomponenten. Gemeinsame Normen für die Beschreibung von Teilnehmern und Diensten gewährleisten jedoch ein gewisses Maß an Kompatibilität: Alle Ökosysteme verstehen die gleichen maschinenlesbaren Metadaten. Ein weiterer Pfeiler der Interoperabilität liegt im gemeinsamen Vertrauensrahmen: Dienste können von der gleichen Behörde zertifiziert werden und die gleichen Compliance-Dienste nutzen. Vertrauensanker für die Identifizierung können ebenfalls gemeinsam genutzt werden, so dass die Teilnehmer in verschiedenen Datenräumen mit denselben Anmeldeinformationen identifiziert werden können.

Interoperabilität ist ein wichtiges Ziel aller Organisationen, die an der Entwicklung einer verteilten Datenwirtschaft beteiligt sind. Europäische Organisationen bemühen sich um die Definition von Möglichkeiten zur Ergänzung der geschäftlichen und technischen Konvergenz sowie der Interaktion zwischen verschiedenen Architekturen (z. B. Gaia-X und IDS[25]). Die Data Spaces Business Alliance (DSBA), die von der Big Data Value Association (BDVA), der FIWARE Foundation, Gaia-X und der International Data Spaces Association (IDSA) gebildet wurde, treibt die Einführung von Datenräumen in ganz Europa voran und hat kürzlich die Entwicklung eines gemeinsamen Rahmens für Datenräume, des Minimum Viable Framework (MVF)[26] initiiert. Auch iSHARE, ein Vertrauensrahmen für Datenräume, hat kürzlich eine Zusammenarbeit mit dem Ziel begonnen, die Vertrauensrahmen von iSHARE und Gaia-X aufeinander abzustimmen. In der Zwischenzeit wurde das Data Spaces Support Centre von der Europäischen Kommission im Rahmen des Programms "Digital Europe" mit dem Ziel finanziert, gemeinsame Datenräume zu erleichtern und einen Datenraumplan zu erstellen.

5 Schlussfolgerung

Offenheit und Zusammenarbeit sind der Schlüssel zu erfolgreichen Datenräumen: Die individuelle technische Umsetzung muss den Bedürfnissen der Teilnehmer:innen entsprechen und mit vereinbarten Regeln und bereichsspezifischen rechtlichen oder geschäftlichen Anforderungen übereinstimmen. Außerdem ist es wichtig, einen Beitrag zur Community zu leisten und die in Datenraumprojekten entwickelte Software als Open Source zu veröffentlichen. 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, offene Communities sowie die technische Konvergenz für eine wirklich offene Datenwirtschaft.

Der Stand der verfügbaren Dataspace-Software ändert sich rasch, um den Anforderungen der zunehmend ausgereiften Initiativen gerecht zu werden. Es zeichnen sich bereits einige dominierende Technologien ab, die sich auf der Grundlage der bewährten Verfahren der ersten Datenraumprojekte zu gemeinsamen Standards entwickeln. Die nächsten technischen Schritte auf dem Weg zu einer breiten Akzeptanz werden einfach zu handhabende Softwarepakete für diejenigen bringen, die ihren eigenen Datenraum hosten wollen, sowie verwaltete Dienste für sofort einsatzbereite Projekte. Der Erwerb eines Konformitätsnachweises und (optional) zusätzlicher Gütesiegel für jedes Angebot wird das Vertrauen in das System stärken, und ein gemeinsamer, verteilter Katalog von Angeboten wird Offenheit und Interoperabilität zwischen verschiedenen Ökosystemen ermöglichen.

6 Glossar

Datenraum

Der Begriff "Datenraum" bezieht sich auf eine Art von Datenbeziehung zwischen vertrauenswürdigen Partnern, die sich an dieselben hohen Standards und Richtlinien für die Speicherung und den Austausch von

Daten halten. Ein entscheidender Aspekt des Datenraumkonzepts 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. Datenräume können verschachtelt sein und sich überschneiden, so dass beispielsweise ein Datenanbieter an mehreren Datenräumen gleichzeitig teilnehmen kann. Datenhoheit und Vertrauen sind wesentliche Voraussetzungen für das Funktionieren von Datenräumen und unterstützen die Beziehungen zwischen den Teilnehmern. Jeder Datenraum stellt spezifische Daten bereit und bildet damit eine solide Grundlage für jedes Ökosystem. Die für die Umsetzung von Datenräumen erforderliche Software läuft auf Cloud-/Edge-Cloud-Infrastrukturen.

Wenn Organisationen eine Gaia-X-Föderation gründen, wird ein zugehöriger Datenraum geschaffen. Gaia-X-kompatible Datenräume erleichtern die Zusammenarbeit zwischen verschiedenen Akteuren und schaffen so Innovationsmöglichkeiten und Wertschöpfung.

Gaia-X Föderation

Der Begriff "Föderation" bezeichnet einen Verbund von mehreren Akteuren, die sich gemeinsam an die Gaia-X-Regeln halten und dieselben Standards und definierten Schnittstellen nutzen, um einen sicheren und souveränen Datenaustausch zu gewährleisten. Eine Föderation beschreibt also auch Transaktionen zwischen verschiedenen IT-Systemen. Sie reduziert unwirtschaftliche Insellösungen und Monopolisierung und unterstützt Interoperabilität und Vertrauensbildung.

Organisationen können vereinbaren, eine beliebige Anzahl von Föderationen zu gründen, die nach Gaia-X-Standards definiert sind. Sie tun dies auf der Grundlage gemeinsam vereinbarter Regeln und mit Hilfe der von Gaia-X bereitgestellten technischen Föderation Services. So können sie ihre IT-Dienste auf vertrauenswürdige Weise miteinander verbinden, um gegenseitig Daten auszutauschen und sie sicher zu nutzen.

IDS Connector

Der Begriff "IDS Connector" bezieht sich auf einen Dienst, der als sicheres Gateway zwischen Einheiten fungiert. Konnektoren sind sowohl für den Datenaustausch untereinander als auch für die Kommunikation mit anderen Datenraumdiensten zuständig. Ein Konnektor kann als Datenaustauschdienst betrachtet werden und verfügt über eine eigene Identität, die im Namen seines Eigentümers im Datenraum registriert werden kann. Ein Konnektor wird in der Regel in der IT-Infrastruktur eines Teilnehmers eingesetzt und kommuniziert mit den internen Datenspeicherdiensten dieses Teilnehmers. Er ist dafür verantwortlich, die Assets des Teilnehmers über seinen internen Katalog dem Datenraum zugänglich zu machen und die Nutzungsrichtlinien festzulegen, die mit diesen Assets verbunden werden können. Der Konnektor wickelt auch die Vertragsverhandlungen im Namen des Teilnehmers ab und orchestriert die Prozesse zur Durchführung des Datentransfers nach dem erfolgreichen Abschluss eines Vertrags.

Überprüfbare Nachweise (Verifiable Credentials)

Der Begriff "verifizierbarer Nachweis" (Variable Credential, VC) bezieht sich auf digitale Zertifikate, die Behauptungen zusammen mit einem kryptografischen Nachweis ihrer Korrektheit enthalten, was sie fälschungssicher und automatisch überprüfbar macht. Der offene W3C-Standard für überprüfbare Nachweise [13] definiert das Datenmodell und Format für VCs. Eine solche VC besteht aus den Metadaten des Ausweises (z. B. Ausstellungsdaten), dem Ausweisgegenstand (die zu überprüfenden Daten) und dem Nachweis (kryptografische Signatur und ihre Metadaten). Es wird die JSON-Syntax für verknüpfte Daten (JSON-LD) verwendet, so dass auch Kontextdaten enthalten sein können, z. B. über die Entität, auf die sich der Berechtigungsnachweis bezieht.

Überprüfbare Nachweise ermöglichen selbstsouveräne Identitäten, bei denen ein Benutzer die volle Kontrolle über seine Identität hat; dies macht sie besonders geeignet für Datenräume. Der Fluss der

überprüfbarer Nachweise („Verifiable Credentials Flow“), der den Prozess der Verwaltung und Verwendung von VCs beschreibt, besteht aus zwei Teilen: einem für die Beschaffung und einem für die Verwendung von VCs. Um eine neue VC zu erhalten, reicht der Besitzer seine Ansprüche („Claims“) bei einem vertrauenswürdigen Aussteller ein, der mit seinem öffentlichen Schlüssel in einem öffentlich zugänglichen, überprüfbareren Datenregister registriert ist. Der Aussteller signiert den Anspruch und sendet ihn an den Eigentümer zurück. Der Eigentümer speichert seine Berechtigungsnachweise, möglicherweise von verschiedenen Ausstellern, in seiner persönlichen Wallet. Wenn ein Dienst vom Eigentümer einen Nachweis für eine bestimmte Behauptung verlangt, kann der Eigentümer eine überprüfbare Darstellung („Verifiable Presentation“) seiner verfügbaren Nachweise erstellen und diese möglicherweise kombinieren und selektiv offenlegen. Der Dienst kann dann diese Darstellung verifizieren, indem er sich die Nachweise ansieht und bestätigt, dass sie tatsächlich von dem vertrauenswürdigen Emittenten signiert wurden, indem er sich dessen Eintrag im verifizierbaren Verzeichnis der Emittenten ansieht.

Im Falle von Datenräumen können die Teilnehmer entscheiden, welche Aussteller sie akzeptieren. Die Gaia-X-Vertrauensdienste fungieren auch selbst als Aussteller, indem sie zum Beispiel Gaia-X-Mitgliedschaftsnachweise für Teilnehmer und Konformitätsnachweise für Dienste ausstellen. Gaia-X-Selbstbeschreibungen sind ebenfalls verifizierbare Nachweise mit Attributen, die durch das Gaia-X Trust Framework [7] beschrieben werden.

7 Danksagung

Wir danken Markus Spiekermann (Fraunhofer ISST) für seinen Beitrag insbesondere zu IDSA und EDC, einschließlich der Grafik zu EDC; Kai Meinke (deltaDAO AG), Thomas Komenda (deltaDAO AG), Meike Molitor (deltaDAO AG), Frederic Schwill (deltaDAO AG) und Albert Peci (deltaDAO AG) für ihren Beitrag insbesondere zu Pontus-X, einschließlich der entsprechenden Architekturabbildung und Vivien Witt (eco - Verband der Internetwirtschaft) für ihren Beitrag insbesondere zu GXFS, einschließlich der dazugehörigen Grafik. Ohne ihren Input zu den diskutierten Technologiestacks wäre dieses Whitepaper nicht möglich gewesen. Wir bedanken uns auch bei Michael Fälbl (Verein Industrie 4.0 Österreich) und Georg Hahn (OSSBIG Österreich) für ihre Review, bei Athina Lyoku (AIT Austrian Institute of Technology) für die Gestaltung der Grafik, die die Grundelemente von Datenräumen zeigt (Abbildung) und bei Agnes Jodkowski (AIT Austrian Institute of Technology) für die deutsche Übersetzung.

Referenzen

- [1] M. Franklin, A. Halevy, and D. Maier, 'From databases to dataspace: a new abstraction for information management', *SIGMOD Rec.*, vol. 34, no. 4, pp. 27-33, Dec. 2005, doi: 10.1145/1107499.1107502.
- [2] 'Home - IDSA', *International Data Spaces*. <https://internationaldataspaces.org/> (Zugriff am 02. Januar 2023).
- [3] B. Otto, S. Steinbuss, A. Teuscher, and S. Lohmann, 'IDS Reference Architecture Model', Zenodo, Apr. 2019. Accessed: Jan. 02, 2023. [Online]. Verfügbar unter: <https://zenodo.org/record/5105529>.
- [4] 'Home - Gaia-X: A Federated Secure Data Infrastructure'. <https://gaia-x.eu/> (Zugriff am 02. Januar 2023).
- [5] "Veröffentlichungen - Gaia-X: A Federated Secure Data Infrastructure". <https://gaia-x.eu/mediatech/publications/> (Zugriff am 06. Januar 2023).
- [6] "Gaia-X Framework". <https://docs.gaia-x.eu/framework/> (Zugriff am 25. Januar 2023).
- [7] "Gaia-X Trust Framework - 22.04 Release". <https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.04/> (Zugriff am 26. Januar 2023).
- [8] 'Introduction - Dataspace Protocol'. <https://docs.internationaldataspaces.org/dataspace-protocol/overview/readme> (Zugriff am 06. März 2023).
- [9] 'Home', *Dataspace Connector*. <https://international-data-spaces-association.github.io/DataspaceConnector/> (Zugriff am 05. Januar 2023).
- [10] 'sovity - The IDS Operating Company', *sovity*. <https://sovity.de/> (Zugriff am 05. Januar 2023).
- [11] "Mobility Data Space - the Data Sharing Community". <https://mobility-dataspace.eu/> (Zugriff am 05. Januar 2023).
- [12] International Data Spaces Association, "Data Connector Report".
- [13] 'Verifiable Credentials Data Model v1.1'. <https://www.w3.org/TR/vc-data-model/> (Zugriff am 05. Januar 2023).
- [14] N. Menz, A. Resetko, and Prof. Dr. B. Otto, 'Framework for the IDS Certification Scheme 2.0', Zenodo, Jan. 2019. doi: 10.5281/zenodo.5244858.
- [15] S. Steinbuss, N. Menz, A. Resetko, and J. Winkel, 'IDS Certification explained', Zenodo, Nov. 2019. doi: 10.5281/zenodo.5675945.
- [16] M. T. Delgado, 'Eclipse Dataspace Components', *projects.eclipse.org*, Jun. 16, 2021. <https://projects.eclipse.org/projects/technology.edc> (Zugriff am 05. Jan. 2023).
- [17] 'Home | Catena-X'. <https://catena-x.net/en/> (Zugriff am 05. Januar 2023).
- [18] "Data-sharing on mobility in Europe", *EONA-X*. <https://eona-x.eu/> (Zugriff am 05. Januar 2023).
- [19] 'Trust Framework Adoption'. Eclipse Dataspace Components, 16. Januar 2023. Accessed: Mar. 06, 2023. [Online]. Verfügbar unter: <https://github.com/eclipse-edc/TrustFrameworkAdoption>
- [20] 'Gaia-X Federation Services', *GXFS.eu*. <https://www.gxfs.eu/> (Zugriff am 02. Januar 2023).
- [21] 'Ocean Protocol Use Case: Gaia-X, eine föderierte europäische Dateninfrastruktur'. *deltaDAO*, 22. September 2022. Aufgerufen: Jan. 25, 2023. [Online]. Available: <https://github.com/deltaDAO/Ocean-Protocol-Use-Cases/blob/3517eeeadc8bbf58626c4611d631179de9c883a6/Ocean%20Protocol%20Use%20Case%20-%20Gaia-X%20v2.pdf>
- [22] 'EuProGigant - EuProGigant'. <https://euprogigant.com/en/> (Zugriff am 10. März 2023).
- [23] 'moveID', *moveID*. <https://moveid.org/> (Zugriff am 10. März 2023).
- [24] "Einführung | GEN-X Netzwerk". <https://docs.genx.minimal-gaia-x.eu/docs/intro/> (Zugriff am 26. Januar 2023).
- [25] Prof. Dr. B. Otto, 'GAIA-X und IDS', Zenodo, Jan. 2021. doi: 10.5281/zenodo.5675897.
- [26] Data Spaces Business Alliance, 'Technical Convergence Discussion Document'. [Online]. Verfügbar unter: <https://data-spaces-business-alliance.eu/dsba-releases-technical-convergence-discussion-document/>

Über den Gaia-X Hub Austria

Beschleunigung der europäischen Datenökosysteme für ökonomische, ökologische und gesellschaftliche Wertschöpfung

Der österreichische Gaia-X Hub wurde im März 2022 auf Initiative des Bundesministeriums für Finanzen (BMF), Staatssekretariat für Digitalisierung, und des Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK) ins Leben gerufen (www.gaia-x.at). Als nationale Gaia-X Anlaufstelle für Unternehmen, öffentliche Einrichtungen und Initiativen soll der Hub die Umsetzung der Gaia-X Strategie in Österreich sicherstellen und damit Datensouveränität als Voraussetzung für nachhaltiges Wirtschaftswachstum und soziale Gerechtigkeit gewährleisten.

Um die Gaia-X Vision effektiv, sichtbar und nachhaltig zu unterstützen, verfolgt der Gaia-X Hub Austria die folgenden vier strategischen Handlungsfelder für alle beteiligten oder interessierten österreichischen Organisationen und Einzelpersonen:

Nr. 1: Informationen bereitstellen, um Vertrauen zu schaffen

Der Gaia-X Hub Austria wird sich als erste Anlaufstelle für Gaia-X in Österreich etablieren. Er wird dafür sorgen, dass alle Arbeitsergebnisse, Richtlinien, Dokumentationen und Open-Source-Codes allen interessierten Stakeholdern in Österreich zeitnah, unkompliziert und verständlich zugänglich gemacht werden.

Nr.2: Erleichterung des Zugangs zur Unterstützung der Entwicklung

Der Gaia-X Hub Austria wird österreichische Organisationen bei der Einführung von datenbasierten Geschäftsmodellen unterstützen und österreichischen Unternehmen aller Größenordnungen die Möglichkeit geben, innovative Umsetzungsprojekte zu initiieren oder sich daran zu beteiligen. Dadurch können sie Erfahrungen sammeln, Know-how erwerben und ihre Wettbewerbsfähigkeit auf dem europäischen Markt steigern.

Nr. 3: Kräfte bündeln, um die Wirksamkeit zu erhöhen

Der Gaia-X Hub Austria wird Organisationen helfen, sich effizient zu vernetzen und unabhängige Arbeitsgruppen und konkrete Allianzen für die Umsetzung zu bilden. Der Hub wird den Zugang zu nationalen und internationalen Förderprogrammen erleichtern und erfolgreiche österreichische Umsetzungsprojekte in anderen EU-Ländern vorstellen. Der Gaia-X Hub Austria wird auch für größtmögliche Synergien mit relevanten österreichischen Initiativen und Programmen sorgen.

Nr. 4: Internationale Vernetzung zur Verbesserung der Sichtbarkeit

Der Gaia-X Hub Austria wird ein starkes Netzwerk mit anderen nationalen Hubs - insbesondere mit jenen der Nachbarländer und osteuropäischen Staaten - aufbauen. Mit dieser starken gemeinsamen Stimme soll sichergestellt werden, dass für Österreich besonders relevante Themen und Fragestellungen auf europäischer Ebene Gehör finden, österreichische Projekte entsprechend präsentiert werden und der österreichische Einfluss auf Entscheidungen zur Datenwirtschaft auf EU-Ebene erhöht wird.

Gaia-X
Innovation durch
digitale Souveränität

info@gaia-x.at
www.gaia-x.at

AIT Österreichisches
Institut für
Technologie GmbH

Gaia-X Europäisch
Vereinigung für Daten
und Cloud AISBL

Ort der Veröffentlichung:
Wien, März 2023

Giefinggasse 4
1210 Wien
Österreich