gaia-x
Hub Austria

GAIA-X HUB AUSTRIA

Europäischer Rechtsrahmen für vertrauenswürdige Datenräume und Gaia-X

Regulatorische Einordnung und technische Relevanz

Gaia-X Summit 2026
Wien, 19. und 20. November 2026



Über das Positionspapier

Regulatorische Einordnung und technische Relevanz

Das vorliegende Positionspapier untersucht die regulatorischen Rahmenbedingungen für die Entwicklung und den Betrieb vertrauenswürdiger, interoperabler und souveräner Datenräume in Europa und analysiert deren Bedeutung für Gaia-X. Im Mittelpunkt stehen acht zentrale europäische Rechtsakte: Datenschutz-Grundverordnung (DSGVO), Data Governance Act, Data Act, eIDAS 2.0, NIS2, Cyber Resilience Act, AI Act und Interoperable Europe Act.

Auf Grundlage einer strukturierten, KI-gestützten Recherche und Vorbewertung werden die Zielsetzungen, relevanten Akteure und wesentlichen Anforderungen der einzelnen Rechtsakte systematisch dargestellt und hinsichtlich ihrer Relevanz für Gaia-X und den österreichischen Datenraumkontext eingeordnet. Ein besonderer Schwerpunkt liegt auf der Verknüpfung regulatorischer Anforderungen mit technischen und organisatorischen Gaia-X-Bausteinen, insbesondere in den Bereichen Vertrauen, Identitätsmanagement, Datensouveränität, Compliance, Sicherheit und Interoperabilität.

Durch die vergleichende Betrachtung werden regulatorische Gemeinsamkeiten, Überschneidungen und potenzielle Umsetzungslücken sichtbar gemacht. Das Positionspapier bietet damit eine strukturierte Orientierung für Unternehmen, öffentliche Einrichtungen, Forschung und weitere Akteure des europäischen Datenökosystems und zeigt auf, wie Gaia-X zur praktischen Umsetzung regulatorischer Anforderungen und zur Etablierung vertrauenswürdiger Datenräume beitragen kann.

REDAKTION

Agnes Jodkowski
AIT Austrian Institute of Technology GmbH / Gaia-X Hub Austria

KONTAKT

Gaia-X Hub Austria
Betrieben von AIT Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Wien, Österreich
info@gaia-x.at www.gaia-x.at

AUTOR:INNEN

Dr. Martin Traunmueller
AIT Austrian Institute of Technology

Dr. Mario Drobics
AIT Austrian Institute of Technology

Juliana Michelon
Gaia-X European Association for Data and Cloud AISBL

Dr. Stephan Winklbauer
AHW Rechtsanwälte Wien

Positionspapier

Inhalt

01	**Einleitung**	**4**
1.1	Hintergrund und Motivation	4
1.2	Zielsetzung und Umfang	4
1.3	Methodischer Ansatz und Abgrenzung	5
02	**Europäischer Rechtsrahmen für Datenräume und Gaia-X**	**6**
2.1	Datenschutz-Grundverordnung (DSGVO/GDPR)	6
2.2	Data Governance Act	7
2.3	Data Act	8
2.4	eIDAS 2 / European Digital Identity Framework	10
2.5	NIS2	11
2.6	Cyber Resilience Act	12
2.7	AI Act	13
2.8	Interoperable Europe Act	14
03	**Zusammenfassende Einordnung**	**14**
	Quellen und weiterführende Hinweise	**16**
A	**Annex A: Vergleichende Übersicht der europäischen Rechtsrahmen**	**17**
B	**Annex B: Gemeinsame regulatorische Anforderungen und Gaia-X-Bausteine**	**18**

01

Einleitung

1.1 Hintergrund und Motivation

Die zunehmende Digitalisierung von Wirtschaft, Verwaltung und Gesellschaft führt zu einem wachsenden Bedarf an einem sicheren, vertrauenswürdigen und interoperablen Austausch von Daten über Organisations-, Sektor- und Ländergrenzen hinweg. Daten bilden eine wesentliche Grundlage für Innovation, Wettbewerbsfähigkeit und neue digitale Dienstleistungen. Zugleich stellen Datensouveränität, Datenschutz, Cybersicherheit und die Zuordnung rechtlicher Verantwortlichkeiten zentrale Herausforderungen für die organisationsübergreifende Datennutzung dar. Die Europäische Union verfolgt daher das Ziel, einen gemeinsamen europäischen Datenmarkt zu etablieren, in dem Daten unter klar definierten rechtlichen, organisatorischen und technischen Bedingungen genutzt werden können.

Eine wesentliche Rolle spielen europäische Datenräume (Common European Data Spaces). Sie ermöglichen den kontrollierten Austausch und die gemeinsame Nutzung von Daten zwischen unterschiedlichen Akteuren, ohne dass diese die Kontrolle über ihre Daten aufgeben müssen. Datenräume stützen sich auf föderierte Architekturen, gemeinsame Standards, interoperable technische Komponenten und Governance-Strukturen. Sie schaffen damit Voraussetzungen für vertrauenswürdige Datenökosysteme, in denen Unternehmen, öffentliche Einrichtungen, Forschungseinrichtungen und weitere Akteure Daten unter definierten Bedingungen bereitstellen und nutzen können.

Gaia-X unterstützt den Aufbau solcher föderierten digitalen Ökosysteme durch gemeinsame technische Spezifikationen, Governance-Prinzipien und überprüfbare Vertrauensmechanismen. Im Mittelpunkt stehen digitale Identitäten, Datensouveränität, Transparenz, Interoperabilität sowie maschinenlesbare Beschreibungen und Nachweise zu digitalen Diensten und Datenangeboten. Gaia-X ist dabei kein eigener Rechtsrahmen und ersetzt keine gesetzlichen Compliance-Verpflichtungen. Vielmehr können seine technischen und organisatorischen Mechanismen dazu beitragen, regulatorische Anforderungen in föderierten Datenökosystemen praktisch umzusetzen.

Der europäische Rechtsrahmen für Datenräume hat sich in den vergangenen Jahren erheblich weiterentwickelt. Mit dem Data Governance Act, dem Data Act, der Datenschutz-Grundverordnung (DSGVO), dem AI Act und Regelungen zu digitalen Identitäten, Cybersicherheit und Interoperabilität wurden wesentliche Voraussetzungen für einen vertrauenswürdigen europäischen Datenaustausch geschaffen oder konkretisiert. Diese Rechtsakte adressieren unterschiedliche, eng miteinander verbundene Aspekte der Datenwirtschaft: Datenzugang und rechtmäßige Nutzung, Identifizierung und Vertrauenswürdigkeit beteiligter Akteure, Sicherheit digitaler Infrastrukturen sowie Nachvollziehbarkeit datenbasierter Prozesse. Sektorale Regelungen, etwa zu digitalen Produktpässen, schaffen zusätzliche Anforderungen an die Bereitstellung und Nutzung von Daten über Organisationsgrenzen hinweg.

Für die Entwicklung und den Betrieb europäischer Datenräume ergibt sich daraus ein komplexes Zusammenspiel regulatorischer Anforderungen, technischer Standards und organisatorischer Verantwortlichkeiten. Einzelne Rechtsakte lassen sich nicht stets isoliert betrachten, da Datenräume häufig mehrere Regelungsbereiche zugleich berühren. Zugleich bieten gemeinsame technische Ansätze wie jene von Gaia-X die Möglichkeit, Identitätsmanagement, Zugriffssteuerung, Datenaustausch und Compliance-Nachweise in unterschiedlichen Anwendungsbereichen wiederzuverwenden.

1.2 Zielsetzung und Umfang

Das folgende Kapitel bietet einen strukturierten Überblick über die wichtigsten europäischen Rechtsakte, die für Datenräume und das Gaia-X-Ökosystem relevant sind. Betrachtet werden ihre Zielsetzungen, Anwendungsbereiche, wesentlichen Anforderungen und Auswirkungen auf technische und organisatorische Datenraumarchitekturen. Ein besonderer Schwerpunkt liegt auf den Wechselwirkungen mit Gaia-X und darauf, inwieweit dessen Spezifikationen und Vertrauensmechanismen die praktische Umsetzung regulatorischer Anforderungen unterstützen können. Dar-

über hinaus wird die Bedeutung der jeweiligen Rechtsakte für österreichische Akteure und den Gaia-X Hub Austria eingeordnet. Ergänzend fasst Annex A die behandelten Rechtsrahmen vergleichend nach Zielsetzungen, Governance-Modellen, technischen Bausteinen und regulatorischen Anforderungen zusammen; Annex B ordnet übergreifende Anforderungen den relevanten Gaia-X-Bausteinen zu und zeigt Konvergenzen sowie Interoperabilitätspotenziale auf.

Ziel ist es, ein gemeinsames Verständnis des regulatorischen Umfelds zu schaffen und Zusammenhänge zwischen rechtlichen Anforderungen, technischen Umsetzungsmöglichkeiten und strategischen Entwicklungen im europäischen Datenökosystem aufzuzeigen. Die Darstellung richtet sich insbesondere an Entscheidungsträger:innen, Datenraum-Initiativen, Technologieanbieter, Unternehmen, öffentliche Einrichtungen und Forschungseinrichtungen. Sie dient der fachlichen Orientierung und ersetzt keine rechtliche Prüfung einzelner Anwendungsfälle.

1.3 Methodischer Ansatz und Abgrenzung

Die Untersuchung folgt einem strukturierten, mehrstufigen Vorgehen, das die systematische Erfassung europäischer Politik- und Regulierungsinitiativen mit einer auf Gaia-X ausgerichteten Bewertung verbindet. Zunächst werden Untersuchungsumfang und Kategorien festgelegt: berücksichtigt werden relevante Rechtsakte, politische Programme, Standards und Initiativen mit Bezug zu vertrauenswürdigem Datenaustausch und föderierten Datenräumen. Ein einheitliches Bewertungsraster erfasst insbesondere Zielsetzung, betroffene Akteure, zentrale Anforderungen sowie die Relevanz für Gaia-X.

Anschließend dient KI-gestützte Webrecherche der Identifikation einschlägiger Initiativen und der Erstellung strukturierter Kurzprofile. Die dabei gewonnenen Angaben sind als Recherche- und Strukturierungshilfe zu verstehen; für belastbare Aussagen werden vorrangig offizielle EU-Rechtsquellen, Veröffentlichungen zuständiger Institutionen sowie einschlägige technische Spezifikationen herangezogen. In einer KI-unterstützten Vorbewertung werden die erfassten Initiativen anhand ihrer Bedeutung für Gaia-X und Österreich sowie ihres Bezugs zu Vertrauen, Compliance und Interoperabilität priorisiert. Die Priorisierung ist eine Orientierungshilfe und ersetzt keine fachliche oder rechtliche Prüfung.

Die so entstandene Auswahl wird im vorgesehenen Verfahren durch ausgewählte Expertinnen und Experten des Gaia-X Hub überprüft, um die Einordnung zu plausibilisieren, Lücken zu identifizieren und gegebenenfalls weitere Initiativen aufzunehmen. Abschließend werden die Ergebnisse thematisch gebündelt sowie Beziehungen, Überschneidungen und gemeinsame Anforderungen herausgearbeitet. Der vorliegende Schwerpunkt liegt auf acht besonders relevanten europäischen Rechtsakten. Die einheitlichen „Snapshots“ in Kapitel 2 verdichten deren Zielsetzung, Adressaten, Kernanforderungen und Gaia-X-Relevanz; Anhang A stellt die Rechtsakte vergleichend gegenüber, während Anhang B gemeinsame Anforderungen technischen Gaia-X-Bausteinen zuordnet.

Die Publikation bietet damit eine regulatorisch-technische Orientierung für das Gaia-X-Ökosystem in Österreich. Sie erhebt weder den Anspruch auf eine vollständige Erfassung aller einschlägigen Initiativen noch auf eine verbindliche juristische Auslegung oder Konformitätsprüfung einzelner Lösungen.

02

Europäischer Rechtsrahmen für Datenräume und Gaia-X

Aufbauend auf dieser Einordnung werden im Folgenden die zentralen europäischen Rechtsakte vorgestellt, die die Entwicklung, den Betrieb und die Nutzung vertrauenswürdiger Datenräume prägen. Die Darstellung folgt den unterschiedlichen regulatorischen Schwerpunkten, vom Schutz personenbezogener Daten und den Bedingungen des Datenzugangs über digitale Identitäten, Cybersicherheit und künstliche Intelligenz bis hin zu Produktinformationen, Interoperabilität und Resilienz. Für jeden Rechtsakt werden die wesentlichen Verpflichtungen und technischen Auswirkungen sowie die möglichen Beiträge von Gaia-X und die Bedeutung für österreichische Akteure eingeordnet. Den Abschluss bildet eine übergreifende Betrachtung des Zusammenspiels dieser Regelungen. Abbildung 1 veranschaulicht die thematische Einordnung der behandelten Rechtsrahmen und ihre gemeinsamen Bezugspunkte für den organisationsübergreifenden Datenaustausch.

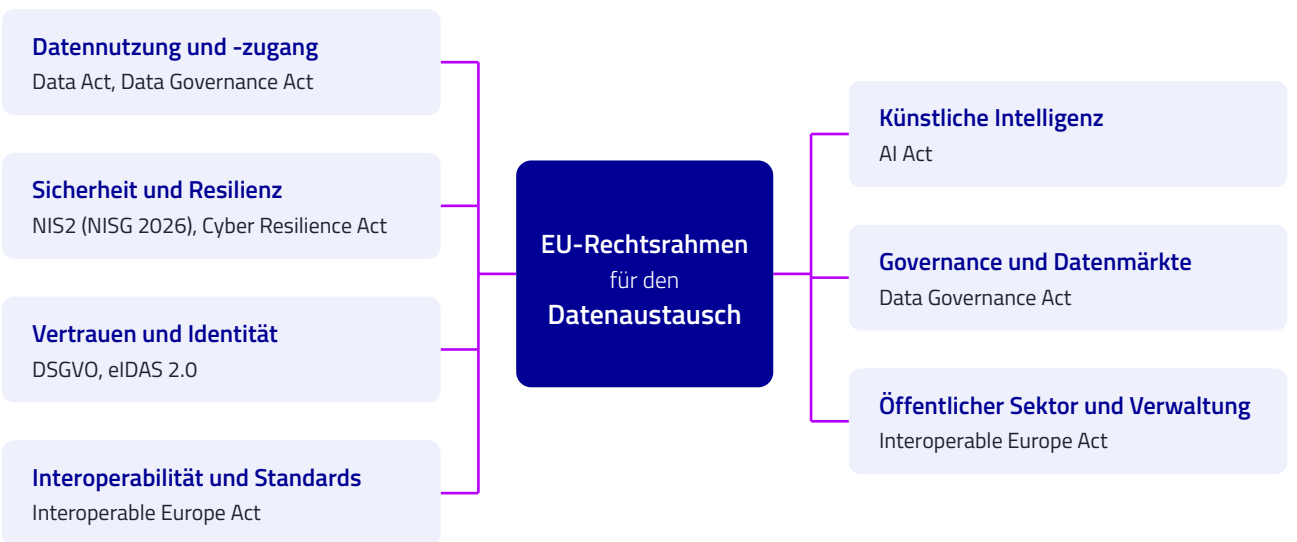

Abbildung 1 Überblick über die relevanten EU-Rechtsrahmen und ihre thematische Einordnung.

2.1 Datenschutz-Grundverordnung (DSGVO/GDPR)

SNAPSHOT

ZIELSETZUNG	ADRESSATEN	KERNANFORDERUNGEN	GAIA-X-RELEVANZ
Schutz personenbezogener Daten	Verantwortliche Auftragsverarbeiter Datenraumbetreiber	Rechtsgrundlage Zweckbindung Sicherheit Betroffenenrechte	Identitäten Zugriffskontrolle Policies Nachweise

Die Datenschutz-Grundverordnung (EU) 2016/679 schafft einen einheitlichen europäischen Rechtsrahmen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und gleichzeitig für den freien Verkehr personenbezogener Daten innerhalb der EU. Die DSGVO gilt grundsätzlich für die automatisierte Verarbeitung personenbezogener Daten durch private und öffentliche Organisationen. Dazu gehören auch personenbezogene Daten, die innerhalb von Datenräumen organisationsübergreifend bereitgestellt, analysiert oder weiterverarbeitet werden. In Österreich wird die DSGVO insbesondere durch das Datenschutzgesetz (DSG) ergänzt. We-

sentliche Anforderungen sind Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht. Hinzu kommen Anforderungen an Privacy by Design und Privacy by Default, Datensicherheit, Betroffenenrechte sowie gegebenenfalls Datenschutz-Folgenabschätzungen.[1]

Für den konkreten Datenaustausch ist insbesondere die Rechtsgrundlage nach Artikel 6 DSGVO zu bestimmen. Bei Auftragsverarbeitung sind Artikel 28, bei technischen und organisatorischen Schutzmaßnahmen Artikel 32 und bei Übermittlungen in Drittstaaten die Vorgaben des Kapitels V zu beachten. In vernetzten Datenökosystemen kann die Abgrenzung personenbezogener und nicht personenbezogener Daten schwierig sein. Gaia-X-Kriterien für Cloud-Dienste können Angaben zu Unterauftragsverarbeitern, Verarbeitungsorten und Sicherheitsmaßnahmen in vergleichbarer Form erfassen; die Prüfung von Rechtsgrundlage, Zweckbindung und Drittlandstransfers bleibt dennoch eine eigenständige Verpflichtung.[1, 16, 21]

AKTEURE

Zu den betroffenen Akteuren zählen Verantwortliche, Auftragsverarbeiter, öffentliche Verwaltungen, Unternehmen, Datenraum-Betreiber, Datenanbieter und -nutzer sowie natürliche Personen als betroffene Personen. Datenräume müssen insbesondere differenzierte Zugriffssteuerung, Identitätsmanagement, Zweck- und Berechtigungsmanagement, Protokollierung und sichere Datenübertragung unterstützen. Technische Architekturen sollten personenbezogene Daten möglichst nicht unnötig vervielfältigen oder zentralisieren. Die DSGVO ist für Datenräume besonders relevant, wenn personenbezogene Daten geteilt werden. Föderierte Architekturen können dabei vorteilhaft sein, weil Daten bei ihren jeweiligen Haltern verbleiben können und der Zugriff kontrolliert erfolgt. Die Europäische Datenstrategie verbindet den europäischen Datenraum ausdrücklich mit hohen Anforderungen an Datenschutz und Datensicherheit.[1]

GAIA-X

Gaia-X unterstützt Prinzipien wie Datensouveränität, überprüfbare Identitäten, kontrollierten Datenzugriff und Policy-basierte Nutzung. Diese Mechanismen können die technische Umsetzung datenschutzkonformer Datenräume unterstützen. Gaia-X-Konformität bedeutet allerdings nicht automatisch DSGVO-Konformität. Ob Daten personenbezogen sind, entscheidet über das anwendbare Regime, lässt sich in vernetzten Umgebungen aber häufig nicht trennscharf beantworten. Für Subverarbeiter, Verarbeitungsorte und getroffene Schutzmaßnahmen fehlt ein standardisierter, prüfbarer Nachweis, den Vertragspartner ohne Einzelaudit verwerten können. Die Gaia-X-Cloud-Kriterien erfassen Angaben zu Auftragsverarbeitung und Unterauftragsverarbeitern sowie zu Verarbeitungsorten und Sicherheitsmaßnahmen. Nachweise können in einem gemeinsamen Format bereitgestellt und entsprechend dem jeweiligen Kriterium geprüft werden. Die Datenaustausch-Kriterien verknüpfen Nutzungsvereinbarungen mit Berechtigungen und Empfängereigenschaften. Das unterstützt die Auswahl von Dienstleistern und die Dokumentation der Verarbeitung. Rechtsgrundlage, Zweckbindung und Zulässigkeit einer Drittlandsübermittlung sind im konkreten Fall zu prüfen; ein Gaia-X-Nachweis ersetzt diese Prüfung nicht.[1, 16, 21]

Für österreichische Gaia-X- und Datenraumprojekte ist die DSGVO eine zentrale Querschnittsanforderung. Besonders relevant ist sie für öffentliche Verwaltung, Gesundheitswesen, Mobilität, Energie, Smart Cities und Forschung. Der Gaia-X Hub Austria kann hier insbesondere Orientierung bei der Verbindung von Datenschutzanforderungen mit föderierten Datenarchitekturen schaffen.[1, 16, 21]

2.2 Data Governance Act

SNAPSHOT

ZIELSETZUNG	ADRESSATEN	KERNANFORDERUNGEN	GAIA-X-RELEVANZ
Vertrauen in freiwilligen Datenaustausch	Öffentliche Stellen Datenvermittler Datenaltruismus	Neutrale Vermittlung Registrierung sichere Weiterverwendung	Identitäten Trust Datenkataloge Compliance

Der Data Governance Act (DGA), Verordnung (EU) 2022/868, soll die Verfügbarkeit von Daten erhöhen und Vertrauen in den freiwilligen Datenaustausch stärken. Er schafft insbesondere Rahmenbedingungen für die Weiterverwendung bestimmter geschützter öffentlicher Daten, Datenvermittlungsdienste und Datenaltruismus. Der DGA betrifft öffentliche Stellen, Datenvermittlungsdienste, Organisationen für Datenaltruismus sowie Unternehmen und Personen, die Daten über solche Mechanismen bereitstellen oder nutzen. Dazu gehören Neutralitäts- und Transparenzanforderungen für Datenvermittlungsdienste, Schutzanforderungen bei der Weiterverwendung sensibler öffentlicher Daten sowie organisatorische und rechtliche Anforderungen für Datenaltruismus.[2]

Der DGA begründet selbst keine allgemeinen Datenzugangsansprüche. Vielmehr ordnet er insbesondere die Rolle neutraler Datenvermittlungsdienste und deren Registrierung beziehungsweise Aufsicht. Eine praktische Herausforderung besteht darin, dass die rechtlich geforderte Neutralität nicht durch einen einheitlichen technischen Nachweis belegt wird. Gaia-X kann hierfür überprüfbare Organisationsidentitäten und standardisierte Dienstbeschreibungen bereitstellen. Amtliche Registrierungen oder Neutralitätsnachweise könnten durch zusätzliche, eigens definierte Aussteller- und Prüfregeln eingebunden werden; eine solche Erweiterung ersetzt die behördlichen Verfahren nicht.[2, 18, 19, 22]

AKTEURE

Zu den betroffenen Akteuren gehören Behörden, Unternehmen, Datenintermediäre, Forschungseinrichtungen, gemeinnützige Organisationen, Datenraum-Betreiber und Dateninhaber. Erforderlich sind sichere Datenaustauschmechanismen, Identitäts- und Berechtigungsmanagement, nachvollziehbare Datenflüsse und gegebenenfalls sichere Verarbeitungsumgebungen. Der DGA ist eine zentrale regulatorische Grundlage für europäische Datenräume. Das vorhandene Gaia-X-Positionspapier bezeichnet DGA und Data Act ausdrücklich als wichtige Rechtsakte, deren Anforderungen besonders durch Datenräume umgesetzt beziehungsweise unterstützt werden können. [2, 18, 19, 22]

GAIA-X

Gaia-X ergänzt den DGA technologisch und organisatorisch. Während der DGA rechtliche Rahmenbedingungen für vertrauenswürdige Datenvermittlung definiert, kann Gaia-X Identitäts-, Trust-, Katalog- und Compliance-Mechanismen bereitstellen. Anwendbar seit 24.09.2023. Neutralität und Vertrauenswürdigkeit sind rechtlich formuliert und behördlich zu überwachen. Ein technischer Nachweis, an dem Marktteilnehmer die Erfüllung ohne eigene Prüfung erkennen, ist nicht vorgesehen.[2, 18, 19, 22]

Gaia-X bietet überprüfbare Organisationsidentitäten und ein gemeinsames Format für Angaben zu Diensten und deren Bedingungen. Damit lassen sich Teilnehmer und Datenvermittler beim Eintritt in einen Datenraum nach einheitlichen Regeln prüfen. Über ergänzende Regeln eines Datenökosystems könnten behördliche Registrierungen oder Nachweise zur Neutralität eingebunden werden, sofern geeignete Aussteller und Prüfverfahren festgelegt sind. Eine solche Erweiterung ist gesondert einzurichten; die Anmeldung und behördliche Überwachung nach dem Data Governance Act bleiben erforderlich. Für Österreich ist der DGA besonders relevant beim Aufbau sektoraler und öffentlicher Datenräume sowie für potenzielle Datenintermediäre. Der Gaia-X Hub Austria kann österreichische Organisationen dabei unterstützen, DGA-Anforderungen mit europäischen Datenraumarchitekturen zu verbinden.[2, 18, 19, 22]

2.3 Data Act

SNAPSHOT

ZIELSETZUNG	ADRESSATEN	KERNANFORDERUNGEN	GAIA-X-RELEVANZ
Fairer Datenzugang und Datennutzung	Hersteller Dateninhaber Nutzer Cloud-Dienste	Zugang Weitergabe Portabilität Interoperabilität	Datenkataloge Policies Nachweise Trust

Der Data Act, Verordnung (EU) 2023/2854, schafft harmonisierte Regeln für einen fairen Zugang zu und die Nutzung von Daten. Ein besonderer Schwerpunkt liegt auf Daten, die durch vernetzte Produkte und verbundene Dienste erzeugt werden. Betroffen sind Hersteller vernetzter Produkte, Anbieter verbundener Dienste, Daten-

halter, Nutzer, Datenempfänger, öffentliche Stellen sowie Anbieter von Datenverarbeitungsdiensten. Der Data Act schafft Rechte von Nutzern auf Zugang zu Produkt- und Nutzungsdaten und deren Weitergabe an Dritte, Regeln für B2B- und B2G-Datenaustausch, Schutz vor unfairen Vertragsbedingungen sowie Anforderungen an den Wechsel zwischen Cloud- und Datenverarbeitungsdiensten und an Interoperabilität.[3]

Für Datenräume sind insbesondere die Kapitel II bis V zum Zugang und zur Weitergabe von Daten, Kapitel VI zum Wechsel von Datenverarbeitungsdiensten und Kapitel VIII zur Interoperabilität relevant; Kapitel VII behandelt den unrechtmäßigen staatlichen Zugriff auf nicht personenbezogene Daten aus Drittstaaten. Artikel 33 formuliert Anforderungen an die Interoperabilität gemeinsamer europäischer Datenräume. Der Data Act ist seit dem 12. September 2025 weitgehend anwendbar; Artikel 3 Absatz 1 betrifft vernetzte Produkte, die ab dem 12. September 2026 in Verkehr gebracht werden, während Wechselentgelte nach Artikel 29 ab dem 12. Januar 2027 entfallen sollen. Für die Konkretisierung der Interoperabilitätsanforderungen wurde am 1. Juli 2025 ein Normungsauftrag der Kommission (C(2025) 4135 final) veröffentlicht. Bis zur Verfügbarkeit einschlägiger harmonisierter Normen verbleiben Unsicherheiten bei Beschreibungs- und Nachweisformaten. Maschinenlesbare Gaia-X-Dienstbeschreibungen, Nutzungsbedingungen und Nachweise können die Umsetzung unterstützen, gewährleisten für sich genommen jedoch keine vollständige Data-Act-Konformität. [3, 17, 20]

AKTEURE

Betroffen sind insbesondere Industrieunternehmen, IoT-Hersteller, Cloud-Anbieter, Plattformen, öffentliche Einrichtungen, KMU, Verbraucher sowie Anbieter und Betreiber von Datenräumen. Daten müssen zunehmend in strukturierten und maschinenlesbaren Formaten bereitgestellt werden. APIs, Interoperabilitätsmechanismen, Datenkataloge, Access Control, Vertrags- und Policy-Management sowie Portabilität gewinnen erheblich an Bedeutung. Datenräume bieten eine mögliche technische Infrastruktur zur Operationalisierung des Data Act. Die vorliegenden Gaia-X-Unterlagen verdeutlichen, dass Datenräume insbesondere Datenzugang, B2B- und B2G-Datenaustausch sowie Anbieterwechsel und Interoperabilität unterstützen können.[3, 17, 20]

GAIA-X

Hier besteht eine besonders enge Verbindung zu Gaia-X: Die Architektur kann verifizierte Identitäten, Trust, Kataloge und Compliance-Mechanismen bereitstellen und dadurch einen kontrollierten und nachvollziehbaren Austausch nach Data-Act-Prinzipien unterstützen. Die zugrunde liegenden Materialien beschreiben Gaia-X-basierte Trust Frameworks und verifizierte souveräne Identitäten als wichtigen Ansatz für sichere Austauschbeziehungen. In Kraft seit 11.01.2024 und in weiten Teilen anwendbar seit 12.09.2025. Art 3 Abs 1 gilt für vernetzte Produkte, die ab 12.09.2026 in Verkehr gebracht werden. Wechselentgelte sinken stufenweise und entfallen ab 12.01.2027 vollständig (Art 29). Die Anforderungen sind abstrakt gefasst. Die konkretisierenden Spezifikationen und harmonisierten Normen liegen nicht vor. Zugang, Portabilität und Interoperabilität sind damit geschuldet, ohne dass ein verbindliches Beschreibungs- und Nachweisformat besteht. Wer heute baut, leistet vor und muss mit Anpassungsaufwand rechnen, sobald die Normung vorliegt.[3, 17, 20]

Gaia-X beschreibt Datenangebote und ihre Anbieter in einem gemeinsamen, maschinenlesbaren Format. Die Vorgaben für Datenaustausch verknüpfen Nutzungsbedingungen mit Berechtigungsnachweisen und dokumentierter Vertragsannahme. Cloud-Kriterien verlangen Transparenz zu Wechsel- und Portierungsverfahren. Damit können Organisationen Angebote vergleichen und Nachweise wiederverwenden. Dies unterstützt die Umsetzung von Zugangsrechten und Interoperabilitätsanforderungen; deren vollständige Erfüllung erfordert zusätzlich geeignete Schnittstellen, Datenmodelle und vertragliche Regelungen. Gaia-X-Konformität ist kein Nachweis der vollständigen Data-Act-Konformität. Der Data Act betrifft zahlreiche österreichische Industrie-, Energie-, Mobilitäts- und IoT-Unternehmen. Für den Gaia-X Hub Austria eröffnet sich insbesondere ein Tätigkeitsfeld bei Data-Act-konformen Datenräumen sowie bei interoperablen Daten- und Cloud-Diensten.[3, 17, 20]

2.4 eIDAS 2 / European Digital Identity Framework

SNAPSHOT

ZIELSETZUNG	ADRESSATEN	KERNANFORDERUNGEN	GAIA-X-RELEVANZ
EU-weit vertrauenswürdige digitale Identitäten	Mitgliedstaaten Vertrauensdienste regulierte Stellen	EUDI-Wallets Identitätsnachweise Attributsattestierungen	Verifiable Credentials Identität Trust

Die Verordnung (EU) 2024/1183 erweitert eIDAS und etabliert einen europäischen Rahmen für digitale Identitäten einschließlich der European Digital Identity Wallet. Ziel ist eine EU-weit nutzbare, sichere und vertrauenswürdige digitale Identifizierung für öffentliche und private Dienste. Der Rahmen betrifft natürliche und juristische Personen, öffentliche Verwaltungen, Trust-Service-Provider und private Dienste, die digitale Identitäten oder elektronische Attribute verwenden. Relevant sind interoperable Wallets, elektronische Identifizierung, qualifizierte Vertrauensdienste sowie die Ausstellung und Verwendung elektronischer Attribute und Nachweise.[4, 18, 19, 22]

Die europäische digitale Identitätsinfrastruktur soll insbesondere elektronische Identitätsnachweise und Attributsattestierungen ermöglichen. Nach dem im zugrunde liegenden Review beschriebenen Zeitplan sollen die Mitgliedstaaten bis Ende 2026 mindestens eine europäische digitale Identitätswallet bereitstellen; für bestimmte private Stellen folgen Akzeptanzpflichten zeitversetzt. Gaia-X ergänzt solche Identitätsnachweise um maschinenlesbare, digital signierte Angaben zu Organisationen und Diensten und nutzt unter anderem Verifiable Credentials sowie OpenID-basierte Austauschmechanismen. Eine Gaia-X-Credential ist jedoch nicht automatisch eine qualifizierte Attributsattestierung im Sinne von eIDAS; hierfür sind geeignete Aussteller, technische Profile und die jeweiligen rechtlichen Voraussetzungen erforderlich.[4, 18, 19, 22]

AKTEURE

Zu den relevanten Akteuren zählen Bürger:innen, Unternehmen, Verwaltung, Identity Provider, Trust-Service-Provider, Datenraum-Betreiber und Anbieter digitaler Dienste. Verifiable Credentials, Wallet-Infrastrukturen, Authentifizierung, Credential Presentation und Interoperabilität zwischen unterschiedlichen Identitätssystemen gewinnen an Bedeutung. Datenräume benötigen zuverlässige Mechanismen zur Identifizierung von Teilnehmern und zur Überprüfung von Rollen, Eigenschaften und Berechtigungen. eIDAS 2 kann hierfür eine europaweit anerkannte Identitätsebene bereitstellen.[4, 18, 19, 22]

GAIA-X

Identity und Trust bilden Kernbestandteile des Gaia-X-Modells. Eine zentrale strategische Schnittstelle besteht daher zwischen European Digital Identity Wallets, elektronischen Attributen und Gaia-X Credentials. Gaia-X kann auf solchen regulierten Identitäts- und Trust-Diensten aufbauen und sie für B2B-Datenökosysteme erweitern. Der Rahmen ist auf Identitätsnachweise natürlicher und juristischer Personen ausgerichtet. Für organisationsbezogene Eigenschaften, die ein Datenraum benötigt, etwa Rolle, Zertifizierungsstand oder Verarbeitungsort, fehlt bisher ein etabliertes Ausstellersystem. Der Vorschlag zu einer europäischen Unternehmensbrieftasche ist noch nicht beschlossen. Gaia-X ergänzt Identitätsnachweise um maschinenlesbare, digital signierte Angaben zu Organisationen und Diensten. Sein Vertrauensmodell berücksichtigt eIDAS-Vertrauensdiensteanbieter und definierte Quellen zur Prüfung von Organisationsdaten. Die Spezifikationen verwenden Verifiable Credentials und OpenID-Protokolle für deren Austausch. So können Identitäten mit zusätzlichen Eigenschaften verknüpft werden. Für solche Eigenschaften müssen vertrauenswürdige Aussteller festgelegt sein. Eine Gaia-X-Credential ist nicht automatisch eine qualifizierte Attributsattestierung; die Anbindung an EUDI-Wallets erfordert die jeweiligen technischen Profile und rechtlichen Voraussetzungen.[4, 18, 19, 22]

Österreich verfügt bereits über eine weit entwickelte staatliche E-ID-Infrastruktur. Für österreichische Gaia-X-Ökosysteme besteht daher besonderes Potenzial, nationale digitale Identitäten mit europäischen Wallet-, Trust- und Datenraummechanismen zu verbinden.[4, 18, 19, 22]

2.5 NIS2

SNAPSHOT

ZIELSETZUNG	ADRESSATEN	KERNANFORDERUNGEN	GAIA-X-RELEVANZ
Hohes gemeinsames Cybersicherheitsniveau	Wesentliche und wichtige Einrichtungen IT-Dienstleister	Risikomanagement Lieferkettensicherheit Meldungen	Trust Sicherheitsnachweise Transparenz

Die NIS2-Richtlinie (EU) 2022/2555 soll ein hohes gemeinsames Cybersicherheitsniveau in der EU schaffen und erweitert den Kreis der verpflichteten Organisationen deutlich. NIS2 umfasst zahlreiche wesentliche und wichtige Einrichtungen etwa in Energie, Verkehr, Gesundheit, digitaler Infrastruktur, öffentlicher Verwaltung, Produktion und weiteren Sektoren. Organisationen müssen Cybersecurity-Risikomanagement etablieren, Sicherheitsmaßnahmen implementieren, Lieferkettenrisiken adressieren, erhebliche Sicherheitsvorfälle melden und Verantwortung auf Managementebene verankern.[5]

Im österreichischen Kontext ist die nationale Umsetzung der NIS2-Anforderungen besonders zu beachten. Die herangezogene regulatorische Übersicht verweist auf das NISG 2026 (BGBl. I Nr. 94/2025) und dessen Inkrafttreten am 1. Oktober 2026. Ein besonderer Schwerpunkt liegt auf der Sicherheit der Lieferkette: Auch kleinere Anbieter können mittelbar betroffen sein, wenn verpflichtete Auftraggeber entsprechende Nachweise verlangen. Standardisierte Informationen über Sicherheitsprüfungen, etwa anhand von ISO/IEC 27001 oder BSI C5, können die wiederholte bilaterale Prüfung erleichtern. Sie ersetzen jedoch weder die eigene Risikobewertung noch Schutzmaßnahmen, Registrierungen oder gesetzliche Meldungen.[5]

AKTEURE

Zu den betroffenen Akteuren gehören Betreiber kritischer und wichtiger Dienste, Cloud- und Rechenzentrumsanbieter, Managed Service Provider, öffentliche Stellen und zahlreiche Industrieunternehmen. Erforderlich sind unter anderem Security Monitoring, Incident Management, Zugriffskontrolle, Business Continuity, Supply-Chain-Security und dokumentierte Sicherheitsmaßnahmen. Datenräume verbinden Organisationen und Systeme über institutionelle Grenzen hinweg. Damit werden sichere Identitäten, sichere Schnittstellen, vertrauenswürdige Teilnehmer und Supply-Chain-Security zentrale Voraussetzungen.[5]

GAIA-X

Gaia-X kann NIS2 unterstützen, indem Eigenschaften von Teilnehmern und Diensten transparent und überprüfbar gemacht werden. Compliance-Nachweise und Trust-Mechanismen können dabei helfen, Sicherheitsanforderungen in föderierten Ökosystemen nachzuweisen; Gaia-X ersetzt jedoch kein NIS2-Risikomanagement. Kundgemacht am 23.12.2025 als BGBl. I Nr. 94/2025 und in Kraft ab 01.10.2026. Die Registrierung ist binnen drei Monaten nach Inkrafttreten vorzunehmen. Ein einheitlicher Nachweis, mit dem ein Zulieferer den Sicherheitsstand gegenüber mehreren Auftraggebern belegt, ist nicht vorgesehen. Der Nachweis erfolgt bilateral über Fragebögen und Audits, was bei einer großen Zahl von Vertragspartnern erheblichen Aufwand auslöst.[5, 16, 21]

Gaia-X kann die Prüfung von Dienstleistern in der Lieferkette erleichtern. Seine Cloud-Kriterien beziehen Sicherheitsanforderungen auf bestehende Prüfstandards, etwa ISO/IEC 27001 oder BSI C5. Vorhandene Nachweise können, soweit das jeweilige Kriterium sie akzeptiert, in die Gaia-X-Prüfung einbezogen und gegenüber mehreren Auftraggebern verwendet werden. Prüfgegenstand und Geltungsbereich müssen erkennbar bleiben. Daraus folgt keine vollständige NISG-Konformität: Die eigene Risikobewertung, die Umsetzung erforderlicher Schutzmaßnahmen und die gesetzlichen Meldepflichten sind gesondert zu erfüllen. NIS2 ist für österreichische Betreiber kritischer und wichtiger Dienste besonders relevant. Das bisherige österreichische NISG wird durch die NIS2-Umsetzung abgelöst; das RIS weist für das bisherige NISG ein Außerkrafttreten mit 30. September 2026 aus. Für Gaia-X Austria sind daher insbesondere Energie, Verkehr, öffentliche Verwaltung und digitale Infrastruktur relevante Zielbereiche.[5, 16, 21]

2.6 Cyber Resilience Act

SNAPSHOT

ZIELSETZUNG	ADRESSATEN	KERNANFORDERUNGEN	GAIA-X-RELEVANZ
Sichere Produkte mit digitalen Elementen	Hersteller Importeure Händler Softwareanbieter	Sichere Entwicklung Schwachstellenmanagement Nachweise	Maschinenlesbare Sicherheitsattribute Trust

Der Cyber Resilience Act, Verordnung (EU) 2024/2847, legt horizontale Cybersecurity-Anforderungen für Produkte mit digitalen Elementen fest und soll sicherstellen, dass Hardware- und Softwareprodukte über ihren Lebenszyklus hinweg angemessen geschützt werden. Erfasst werden grundsätzlich Produkte mit digitalen Elementen, einschließlich Hardware und Software, die auf dem EU-Markt bereitgestellt werden. Security by Design, sichere Standardkonfigurationen, Umgang mit Schwachstellen, Sicherheitsupdates, technische Dokumentation und Meldepflichten gehören zu den zentralen Elementen.[6]

Der CRA sieht gestaffelte Anwendungsfristen vor: Meldepflichten nach Artikel 14 gelten nach der zugrunde gelegten regulatorischen Übersicht ab dem 11. September 2026; die umfassenden Produktanforderungen einschließlich Konformitätsbewertung und CE-Kennzeichnung ab dem 11. Dezember 2027. Zu den Anforderungen an den Umgang mit Schwachstellen gehört eine Software Bill of Materials (SBOM), die Komponenten eines Produkts in einem gängigen maschinenlesbaren Format dokumentiert. Für einen organisationsübergreifenden Austausch solcher Nachweise können föderierte Datenräume nützlich sein. Gaia-X könnte Produktversionen, signierte Nachweise und Verweise auf SBOMs miteinander verknüpfen; ein eigenes SBOM-Format oder ein CRA-Konformitätsverfahren stellt Gaia-X damit nicht bereit.[7, 15, 17]

AKTEURE

Zu den betroffenen Akteuren gehören Hersteller, Importeure, Händler, Softwareanbieter sowie Betreiber und Nutzer digitaler Produkte. Secure Development Lifecycle, Vulnerability Management, Software-Update-Prozesse, Dokumentation und Nachweisführung müssen systematisiert werden. Konnektoren, Softwarekomponenten, IoT-Geräte und andere Produkte können Teil eines Datenraumökosystems sein. CRA-Konformität erhöht somit die Sicherheit der technischen Basis von Datenräumen.[6]

GAIA-X

Gaia-X könnte CRA-bezogene Konformitäts- oder Sicherheitseigenschaften eines Produktes oder Services als maschinenlesbare Trust-Information abbilden. Dadurch entsteht eine Verbindung zwischen Produktsicherheit und der Gaia-X-basierten Bewertung vertrauenswürdiger digitaler Ressourcen. In Kraft seit 10.12.2024. Die Meldepflichten nach Art 14 für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle gelten ab 11.09.2026, mit Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden und Abschlussbericht binnen 14 Tagen. Ab 11.12.2027 gelten die vollständigen Produktanforderungen einschließlich Konformitätsbewertung und CE-Kennzeichnung. Format und Austauschweg der SBOM über die Lieferkette hinweg sind nicht abschließend vorgegeben. Für weitere Produkt- und Komponenteneigenschaften, die Abnehmer benötigen, fehlt eine einheitliche prüfbare Darstellung.[7, 15, 17]

Gaia-X kann einen geregelten Austausch von Software-Stücklisten und Produktnachweisen zwischen identifizierten Lieferkettenpartnern unterstützen. Dafür können die Datenaustauschmechanismen zur Vereinbarung von Nutzungsbedingungen und Berechtigungen eingesetzt werden. Eine CRA-bezogene Erweiterung könnte Produktversionen mit signierten Nachweisen und Verweisen auf SBOMs verbinden. Entsprechende Datenmodelle, Aussteller und Prüfregeln müssten dafür festgelegt werden. Gaia-X stellt kein eigenes SBOM-Format und kein CRA-Konformitätsverfahren bereit; Produktprüfungen, Schwachstellenmanagement und Behördenmeldungen bleiben gesonderte Aufgaben. Der CRA ist insbesondere für österreichische Software-, IoT-, Automatisierungs- und Industrieunternehmen relevant. Für Gaia-X Austria ergibt sich daraus ein mögliches Handlungsfeld rund um digitale Compliance Credentials und automatisierte Nachweisführung an.[7, 15, 17]

2.7 AI Act

SNAPSHOT

ZIELSETZUNG	ADRESSATEN	KERNANFORDERUNGEN	GAIA-X-RELEVANZ
Sichere und vertrauenswürdige KI-Systeme	KI-Anbieter Betreiber Datenanbieter	Daten-Governance Dokumentation Protokollierung	Datenherkunft Nutzungsrechte Trust Nachweise

Der AI Act, Verordnung (EU) 2024/1689, schafft harmonisierte Regeln für künstliche Intelligenz und soll sichere und vertrauenswürdige KI-Systeme fördern, während Gesundheit, Sicherheit und Grundrechte geschützt werden. Der AI Act umfasst Anbieter, Betreiber und weitere Akteure entlang der AI-Wertschöpfungskette. Die regulatorischen Anforderungen richten sich nach Art und Risiko des jeweiligen AI-Systems. Für regulierte Systeme können insbesondere Risikomanagement, Data Governance, technische Dokumentation, Logging, Transparenz, Human Oversight, Robustheit und Cybersecurity erforderlich sein. [7]

Für den Datenaustausch sind besonders Artikel 10 zur Daten-Governance, Artikel 11 zur technischen Dokumentation, Artikel 12 zur Protokollierung, Artikel 25 zur Pflichtenverteilung in der Wertschöpfungskette und Artikel 53 zu Modellen mit allgemeinem Verwendungszweck relevant. Nach dem zugrunde liegenden Review gelten Anforderungen an KI-Kompetenz und bestimmte Verbote seit dem 2. Februar 2025 sowie Pflichten für Modelle mit allgemeinem Verwendungszweck seit dem 2. August 2025. Die zugrunde gelegte Übersicht berücksichtigt außerdem die Verordnung (EU) 2026/1744 und nennt den 2. Dezember 2027 für eigenständige Hochrisikosysteme nach Anhang III. Die Herkunft und zulässige Verwendung von Trainingsdaten können durch überprüfbare Datenproduktbeschreibungen und Transaktionsnachweise unterstützt werden. Eine Bewertung der Dateneignung sowie die KI-spezifischen Dokumentations- und Risikomanagementpflichten bleiben davon unabhängig.[7]

AKTEURE

Betroffen sind KI-Anbieter, Betreiber, Datenanbieter, Forschungseinrichtungen, öffentliche Stellen, Cloud- und Computing-Anbieter. Datenherkunft, Datenqualität, Dokumentation, Logging, Model Governance und nachvollziehbare KI-Pipelines gewinnen an Bedeutung. Datenräume können vertrauenswürdige und kontrollierbare Datenquellen für AI bereitstellen. Sie ermöglichen zudem die organisationsübergreifende Nutzung von Trainings-, Validierungs- und Betriebsdaten unter definierten Bedingungen. [7]

GAIA-X

Ein Gaia-X-Synergiepapier beschreibt AI als besonders geeignetes Anwendungsfeld des Gaia-X Trust Framework: hochwertige Daten, Algorithmen und Computing-Ressourcen können über föderierte vertrauenswürdige Ökosysteme bereitgestellt werden. In Kraft seit 01.08.2024. Verbotene Praktiken und die Anforderungen an KI-Kompetenz gelten seit 02.02.2025, die Pflichten für Modelle mit allgemeinem Verwendungszweck seit 02.08.2025. Die Digital-Omnibus-Verordnung zur Künstlichen Intelligenz, VO (EU) 2026/1744, wurde am 24.07.2026 verkündet und ist seit 27.07.2026 in Kraft. Eigenständige Hochrisikosysteme nach Anhang III unterliegen den Pflichten ab 02.12.2027. Die Verordnung verlangt Dokumentation, gibt aber kein Format für einen anbieterübergreifenden Herkunftsnachweis vor. Das Fehlen fertiger harmonisierter Normen nach Art 40 war einer der Gründe für die Verschiebung der Fristen für Hochrisikosysteme.[8, 17, 20]

Gaia-X kann die Beschaffung von Daten für KI-Anwendungen unterstützen: Beschreibungen von Datenprodukten verknüpfen Anbieter und Nutzungsrechte mit überprüfbaren Nachweisen. Die Datenaustausch-Spezifikationen berücksichtigen die Protokollierung von Transaktionen. Daraus können Belege für die Herkunft und zulässige Nutzung bezogener Daten entstehen. Für KI-spezifische Qualitätskriterien wären ergänzende Regeln und Prüfverfahren erforderlich. Die Eignung eines Datensatzes für ein konkretes KI-System sowie die Erfüllung der Dokumentations- und Risikomanagementpflichten müssen separat bewertet werden. Österreich verfügt über starke industrielle AI-, Forschungs- und Public-Sector-Ökosysteme. Gaia-X Austria kann insbesondere vertrauenswürdige KI-Datenräume, Datenherkunft und Zugang zu föderierten Computing-Ressourcen adressieren.[8, 17, 20]

2.8 Interoperable Europe Act

SNAPSHOT

ZIELSETZUNG	ADRESSATEN	KERNANFORDERUNGEN	GAIA-X-RELEVANZ
Grenzüberschreitende Interoperabilität im öffentlichen Sektor	Behörden EU-Institutionen öffentliche IT-Dienste	Interoperabilitätsbewertungen gemeinsame Lösungen	Föderation Dienstbeschreibungen Trust

Der Interoperable Europe Act, Verordnung (EU) 2024/903, soll ein hohes Niveau grenzüberschreitender Interoperabilität im öffentlichen Sektor der EU schaffen. Er betrifft EU-Institutionen und öffentliche Stellen der Mitgliedstaaten, insbesondere bei grenzüberschreitenden digitalen öffentlichen Diensten. Wesentliche Elemente sind Interoperabilitätsbewertungen, gemeinsame Governance, Wiederverwendung interoperabler Lösungen und Unterstützung gemeinsamer europäischer Lösungen.[8]

Für grenzüberschreitend relevante öffentliche digitale Dienste können Interoperabilitätsbewertungen vor Einführung oder wesentlicher Änderung von Netz- und Informationssystemen erforderlich werden. Einheitliche Dienstbeschreibungen und überprüfbare Eigenschaften, wie sie Gaia-X unterstützt, können Vergleich und Dokumentation erleichtern. Die gesetzliche Bewertung sowie die Abstimmung fachlicher Datenmodelle und organisatorischer Zuständigkeiten müssen die zuständigen öffentlichen Stellen selbst vornehmen.[11, 18, 19, 22]

AKTEURE

Dies betrifft Ministerien, Behörden, Länder, Gemeinden, EU-Institutionen und öffentliche IT-Dienstleister. Offene Schnittstellen, gemeinsame Datenmodelle und wiederverwendbare Komponenten stärken dabei die technische, semantische und organisatorische Interoperabilität.[8]

GAIA-X

Gaia-X kann Trust und Federation zwischen öffentlichen und privaten Teilnehmern ergänzen. Besonders interessant sind Anwendungen, bei denen öffentliche Daten mit Unternehmensdaten oder Forschungsdaten verbunden werden. Die Bewertung setzt beschreibbare Systeme und vergleichbare Beschreibungsformate voraus. Beides gibt der Rechtsakt nicht vor. Gaia-X bietet gemeinsame Beschreibungsmodelle für Organisationen und digitale Dienste sowie überprüfbare Angaben zu deren Bedingungen. Öffentliche Stellen können diese Informationen für den Vergleich von Angeboten und die Dokumentation organisationsübergreifender Datenaustauschbeziehungen nutzen. Der Beitrag liegt vor allem bei der technischen und semantischen Verständigung über Identitäten und Nachweise. Diese Informationen können eine Interoperabilitätsbewertung unterstützen. Die gesetzlich verlangte Bewertung und die Abstimmung fachlicher Datenmodelle sowie rechtlicher und organisatorischer Voraussetzungen bleiben Aufgaben der beteiligten öffentlichen Stellen.[11, 18, 19, 22]

Der Act ist für Bund, Länder und Gemeinden relevant und passt unmittelbar zu österreichischen Smart-City-, Verwaltungs- und kommunalen Datenraumaktivitäten. Für Gaia-X Austria ist dies daher ein strategisch relevantes Public-Sector-Thema.[11, 18, 19, 22]

03
Zusammenfassende Einordnung

Die acht in Kapitel 2 dargestellten Rechtsakte bilden keinen einheitlichen Rechtsrahmen für Datenräume, sondern ergänzen sich in ihren Anforderungen an Datenschutz, Datenzugang, Governance, Identität, Cybersicherheit, KI und Interoperabilität. Für Gaia-X ergeben sich daraus technische und organisatorische Anknüpfungspunkte, ohne dass Gaia-X-Konformität die Erfüllung einzelner gesetzlicher Pflichten ersetzt.

Für Gaia-X liegt die strategische Bedeutung vor allem in der Bereitstellung wiederverwendbarer Vertrauens- und Interoperabilitätsmechanismen. Überprüfbare Organisationsidentitäten, maschinenlesbare Beschreibungen von

Datenangeboten und digitalen Diensten, nachvollziehbare Nutzungsbedingungen sowie definierte Verfahren zur Bewertung von Nachweisen können den Austausch zwischen bislang getrennten Akteuren erleichtern. Solche gemeinsamen Bausteine lassen sich über Sektoren und Anwendungsfälle hinweg einsetzen und mit spezifischen Anforderungen eines Datenökosystems ergänzen. Die technische Unterstützung durch Gaia-X ist jedoch klar von der rechtlichen Erfüllung einzelner Verpflichtungen zu unterscheiden: Ein Gaia-X-Nachweis oder die Erfüllung bestimmter Kriterien begründet für sich genommen keine umfassende Konformität mit DSGVO, Data Act, NIS2 oder anderen Rechtsakten.[15, 16, 17, 18, 19, 22]

Die praktische Umsetzung sollte deshalb von den Rollen und Datenaustauschbeziehungen ausgehen. Eine Organisation kann zugleich Dateninhaberin, Datennutzerin, Betreiberin eines Datenraums, Anbieterin eines Datenverarbeitungsdienstes oder Betreiberin eines KI-Systems sein. Für jede dieser Rollen sind die einschlägigen Rechte, Pflichten und vertraglichen Beziehungen zu klären. Drei Fragen bieten dafür einen übergreifenden Ausgangspunkt: Wer ist das Gegenüber und wie werden dessen Eigenschaften nachgewiesen? In welcher Form können Daten technisch und semantisch interoperabel ausgetauscht werden? Unter welchen rechtlichen, vertraglichen und organisatorischen Bedingungen ist die Nutzung zulässig? Die Antworten bestimmen, welche Identitäts-, Policy-, Schnittstellen- und Nachweismechanismen tatsächlich erforderlich sind.[2, 3, 8, 23]

Ein besonderes Handlungsfeld ist die Nachweisfähigkeit. Mehrere Rechtsakte verlangen dokumentierte Sicherheitsmaßnahmen, Datenherkunft, Nutzungsrechte oder die Einhaltung bestimmter Verfahren, ohne für sämtliche organisationsübergreifenden Nachweise ein einheitliches technisches Format festzulegen. Gaia-X kann hier die strukturierte Bereitstellung und Prüfung definierter Eigenschaften unterstützen und vorhandene Zertifizierungen oder Erklärungen in interoperable Vertrauensprozesse einbinden. Welche Nachweise akzeptiert werden, wer sie ausstellen darf und wie ihre Gültigkeit überprüft wird, muss jedoch für den jeweiligen Anwendungsfall festgelegt werden. Ebenso bleiben rechtliche Einzelfallprüfungen, behördliche Verfahren und die Verantwortung der beteiligten Organisationen bestehen.[16, 17, 21]

Für den Gaia-X Hub Austria ergibt sich daraus eine vermittelnde und koordinierende Rolle zwischen europäischer Regulierung, technischen Spezifikationen und österreichischen Datenrauminitiativen. Ein strategischer Schwerpunkt kann darin liegen, regulatorische Anforderungen in konkrete technische und organisatorische Anforderungen zu übersetzen, wiederverwendbare Trust- und Compliance-Bausteine sichtbar zu machen und sektorübergreifende Synergien zu fördern. Besonders anschlussfähig sind industrielle Lieferketten und digitale Produktpässe, Energie- und Mobilitätsdatenräume, öffentliche und kommunale Datenökosysteme sowie Anwendungsfälle rund um kritische Infrastrukturen und vertrauenswürdige KI. Dabei sollten bestehende nationale Infrastrukturen und europäische Standards berücksichtigt werden, um parallele Insellösungen zu vermeiden.[15, 18, 19, 22]

Für die weitere Entwicklung eines österreichischen Policy & Initiative Radar folgt daraus ein kontinuierlicher Beobachtungs- und Übersetzungsauftrag. Neben dem Stand und den Anwendungsfristen der Rechtsakte sind insbesondere Durchführungsrechtsakte, harmonisierte Normen, technische Spezifikationen und neue Nachweisverfahren relevant. Ein solcher Radar kann Änderungen frühzeitig sichtbar machen, ihre Auswirkungen auf konkrete Datenraumrollen und Architekturen einordnen und daraus priorisierte Handlungsfelder für österreichische Akteure ableiten. Der Mehrwert von Gaia-X liegt damit nicht in einer pauschalen Compliance-Zusage, sondern darin, vertrauenswürdigen und interoperablen Datenaustausch unter sich weiterentwickelnden regulatorischen Bedingungen praktisch zu unterstützen.[15, 20, 23]

Quellen und weiterführende Hinweise

Die nachfolgende Auswahl umfasst die im Paper behandelten EU-Rechtsakte sowie die in den zugrunde liegenden Unterlagen angeführten Gaia-X-Dokumente. Rechtsakte sind über EUR-Lex anhand ihrer offiziellen Nummer auffindbar. Die Links zu Gaia-X-Spezifikationen verweisen auf die im Review angeführten Dokumentationsseiten.

[1] Europäische Union (2016): Datenschutz-Grundverordnung (DSGVO), Verordnung (EU) 2016/679.

[2] Europäische Union (2022): Data Governance Act, Verordnung (EU) 2022/868.

[3] Europäische Union (2023): Data Act, Verordnung (EU) 2023/2854.

[4] Europäische Union (2024): European Digital Identity Framework (eIDAS 2), Verordnung (EU) 2024/1183.

[5] Europäische Union (2022): NIS2-Richtlinie, Richtlinie (EU) 2022/2555.

[6] Europäische Union (2024): Cyber Resilience Act, Verordnung (EU) 2024/2847.

[7] Europäische Union (2024): Artificial Intelligence Act, Verordnung (EU) 2024/1689; im Review genannte Änderung: Verordnung (EU) 2026/1744.

[8] Europäische Union (2024): Interoperable Europe Act, Verordnung (EU) 2024/903.

[9] Gaia-X AISBL (2025): Gaia-X Synergies with prominent European data, cloud and digital policy initiatives & projects, Version 1.0, Dezember 2025.

[10] Gaia-X: Compliance Document, Criteria for Cloud Services. docs.gaia-x.eu/policy-rules-committee/compliance-document/latest/criteria_cloud_services

[11] Gaia-X: Compliance Document, Criteria for Data Exchange Services. docs.gaia-x.eu/policy-rules-committee/compliance-document/latest/criteria_data_exchange_services

[12] Gaia-X: Compliance Document, Trust Anchors. docs.gaia-x.eu/policy-rules-committee/compliance-document/latest/Gaia-X_Trust_Anchors

[13] Gaia-X: Compliance Document, Criteria for General Digital Services. docs.gaia-x.eu/policy-rules-committee/compliance-document/latest/criteria_digital_services

[14] Gaia-X: Data Exchange Services, Glossary (25.11). docs.gaia-x.eu/glossary/25.11/data_exchange_services

[15] Gaia-X: Compliance Document, Criteria Assessment Methods. docs.gaia-x.eu/policy-rules-committee/compliance-document/latest/criteria_assessment_methods

[16] Gaia-X: Identity, Credential and Access Management Document (25.11). docs.gaia-x.eu/technical-committee/identity-credential-access-management/25.11/standards

[17] European Regulations and Data Exchange, Review JM (26.10.2026), bereitgestelltes Review-Dokument; ergänzende redaktionelle Grundlage.

Hinweis: Die Zusammenstellung basiert auf den bereitgestellten Dokumenten. Aktualität, Geltungsstände und einzelne Rechtsverweise wurden nicht unabhängig juristisch geprüft.

Annex A

Vergleichende Übersicht der europäischen Rechtsrahmen

Die folgende Übersicht verdichtet die in Kapitel 2 behandelten Rechtsrahmen entlang ihrer Zielsetzungen, Governance-Modelle, technischen Bausteine und regulatorischen Anforderungen. Die letzte Spalte benennt wesentliche Konvergenzen, Überschneidungen und Interoperabilitätspotenziale. Die Aussagen sind als komprimierte Orientierung zu verstehen; der Digital Product Passport ist ein regulatorisches Instrument und kein eigenständiger Rechtsakt.

Rechtsrahmen	Zielsetzungen & Governance	Technische Bausteine	Regulatorische Anforderungen	Konvergenz, Überschneidung & Interoperabilität
2.1 DSGVO	Schutz personenbezogener Daten; freier Datenverkehr Verantwortliche und Auftragsverarbeiter; Betroffenenrechte	Zugriffskontrolle; Pseudonymisierung; Protokollierung	Rechtsgrundlage; Zweckbindung; Datenminimierung; Sicherheit	Gemeinsame Identitäts- und Zugriffsebene; kumulativ mit Data Act
2.2 Data Governance Act	Vertrauen in freiwillige Datenteilung; Wiederverwendung geschützter öffentlicher Daten Neutrale Datenvermittler; registrierte Dienste; Datenaltruismus	Identitätsprüfung; Berechtigungen; sichere Verarbeitungsumgebungen	Neutralität; Transparenz; Anmeldung und Aufsicht	Vertrauensnachweise ergänzen Gaia-X; keine eigenen Zugangsansprüche
2.3 Data Act	Fairer Datenzugang; Weitergabe; Cloud-Wechsel Dateninhaber, Nutzer, Empfänger und Cloud-Anbieter; B2G-Ausnahmen	APIs; Datenmodelle; Portabilität; Kataloge	Zugangsrechte; Vertragsfairness; Interoperabilität; Wechselpflichten	Art. 33 mit Datenraum-Interoperabilität; Ergänzung zu DSGVO/DGA
2.4 eIDAS 2	EU-weit vertrauenswürdige digitale Identitäten und Attribute Mitgliedstaaten; Wallet-Anbieter; Vertrauensdienste	EUDI-Wallet; Verifiable Credentials; Attributsnachweise	Anerkennung und Akzeptanz digitaler Identitäten; Vertrauensdienste	Identitätsbasis für Gaia-X; Gaia-X-Credentials nicht automatisch qualifiziert
2.5 NIS2	Hohes gemeinsames Cybersicherheitsniveau Wesentliche und wichtige Einrichtungen; Managementverantwortung	Monitoring; Incident Management; Zugriffsschutz; Business Continuity	Risikomanagement; Lieferkettensicherheit; Meldepflichten	Sicherheitsnachweise für Teilnehmer; Ergänzung zu CRA und CER
2.6 Cyber Resilience Act	Sicherheit von Produkten mit digitalen Elementen Hersteller; Einführer; Händler	Secure Development; Schwachstellenmanagement; SBOM; Updates	Security by Design; Dokumentation; Meldungen; Konformitätsbewertung	SBOM-/Produktnachweise über Datenräume austauschbar; NIS2 komplementär
2.7 AI Act	Sichere, grundrechtskonforme und vertrauenswürdige KI Anbieter; Betreiber; Akteure der KI-Wertschöpfungskette	Datenprovenienz; Logging; Modell- und Datendokumentation	Risikomanagement; Daten-Governance; Transparenz; Aufsicht	Datenräume unterstützen Nachweise; keine automatische KI-Konformität

Rechtsrahmen	Zielsetzungen & Governance	Technische Bausteine	Regulatorische Anforderungen	Konvergenz, Überschneidung & Interoperabilität
2.8 Interoperable Europe Act	Grenzüberschreitende Interoperabilität öffentlicher Dienste Öffentliche Stellen; gemeinsame europäische Governance	Offene Schnittstellen; semantische Modelle; wiederverwendbare Lösungen	Interoperabilitätsbewertungen; Kooperation; Wiederverwendung	Anschluss öffentlicher Datenräume an Gaia-X-Vertrauensmechanismen

Hinweis: Die technischen Bausteine beschreiben mögliche beziehungsweise naheliegende Umsetzungsmechanismen und sind nicht in jedem Fall unmittelbar gesetzlich vorgeschrieben. Gaia-X unterstützt die technische Nachweisführung, ersetzt jedoch keine rechtsaktspezifische Konformitätsprüfung.

Annex B

Gemeinsame regulatorische Anforderungen und Gaia-X-Bausteine

Die folgende Zuordnung bündelt wiederkehrende Anforderungen aus den in Kapitel 2 und Annex A beschriebenen europäischen Rechtsrahmen und stellt ihnen mögliche Gaia-X-Bausteine gegenüber. Sie dient als Orientierung für die Konzeption föderierter Datenräume. Die genannten Gaia-X-Mechanismen unterstützen die technische und organisatorische Umsetzung; sie begründen für sich genommen weder Rechtskonformität noch eine Zertifizierung.

Gemeinsame Anforderung	Rechtsrahmen (Kap. 2)	Mögliche Gaia-X-Bausteine	Konvergenz / Interoperabilität	Abgrenzung / Umsetzungsbedarf
Identität und Authentifizierung	DSGVO (2.1) eIDAS 2 (2.4) NIS2 (2.5)	Gaia-X Identity, Credential and Access Management (ICAM) Verifizierbare Identitäts- und Organisationsnachweise	Einheitliche Prüfung von Akteuren und Rollen Föderationsübergreifende Vertrauensbeziehungen	Identitätsnachweise sind nicht automatisch eIDAS-qualifiziert; Schutzbedarf und Identitätsniveau sind kontextspezifisch.
Zugriffsrechte und Datennutzung	DSGVO (2.1) Data Act (2.3) DGA (2.2)	ICAM und Autorisierung Data Exchange Services; maschinenlesbare Nutzungsbedingungen	Rollen- und zweckgebundene Freigaben Durchsetzung von Nutzungsbedingungen an Austauschpunkten	Rechtsgrundlagen, gesetzliche Zugangsrechte und vertragliche Bedingungen müssen gesondert geprüft werden.
Transparenz und überprüfbare Nachweise	DGA (2.2) AI Act (2.7) Data Act (2.3)	Gaia-X Compliance Document Trust Anchors Nachweise/Attestierungen und Kriterienprüfung	Nachvollziehbare Aussagen zu Diensten und Akteuren Wiederverwendbare Evidenz für Partnerprüfungen	Gaia-X-Compliance ist kein Ersatz für gesetzlich vorgeschriebene Prüfungen oder Konformitätsbewertungen.
Cybersicherheit und Resilienz	NIS2 (2.5) CRA (2.6)	Vertrauenswürdige Identitäten und Zugriffssteuerung Nachweisbare Sicherheitsmerkmale digitaler Dienste	Gemeinsame Mindestanforderungen an vertrauenswürdige Dienste Austausch sicherheitsbezogener Evidenz	Vorfallmeldung, Produktsicherheit, operative Resilienz und Zertifizierung haben unterschiedliche Adressaten und Pflichten.
Interoperabilität und Datenportabilität	Data Act (2.3) Interoperable Europe Act (2.8)	Gaia-X Data Exchange Services Gemeinsame Beschreibungen, Schnittstellen und Metadaten	Föderierter Datenaustausch über Organisationsgrenzen Anschlussfähigkeit unterschiedlicher Datenräume	Fachliche Datenmodelle, sektorale Standards und öffentliche Interoperabilitätsvorgaben bleiben zusätzlich erforderlich.

Gemeinsame Anforderung	Rechtsrahmen (Kap. 2)	Mögliche Gaia-X-Bausteine	Konvergenz / Interoperabilität	Abgrenzung / Umsetzungsbedarf
Datenherkunft und Rückverfolgbarkeit	AI Act (2.7) DSGVO (2.1)	Verifizierbare Nachweise und Beschreibungen Vertrauensanker und dokumentierte Datenflüsse	Prüfung von Herkunft und Verantwortlichkeiten Wiederverwendbare Nachweisketten	Produktpass-, KI- und Datenschutzpflichten verlangen jeweils eigene fachliche Inhalte und Dokumentation.
Governance und Rollenverteilung	DGA (2.2) DSGVO (2.1) Interoperable Europe Act (2.8)	Gaia-X Compliance-Kriterien Rollen-, Teilnehmer- und Dienstebeschreibungen	Transparente Verantwortlichkeiten in föderierten Ökosystemen Gemeinsame Onboarding-Regeln	Gesetzliche Rollen (z. B. Verantwortlicher, Datenvermittlungsdienst) werden nicht durch Gaia-X-Rollen ersetzt.
Vertrauenswürdige digitale Dienste	eIDAS 2 (2.4) NIS2 (2.5) CRA (2.6)	Gaia-X Trust Anchors Compliance-Kriterien für digitale und Cloud-Dienste	Einheitliche Prüfung von Dienstmerkmalen Vertrauensbasierte Zusammenarbeit	Gaia-X-Kriterien sind von formalen EU-Zertifizierungen und qualifizierten Vertrauensdiensten zu unterscheiden.

Einordnung: Besonders ausgeprägte Schnittmengen bestehen bei Identitäts- und Vertrauensmanagement, Zugriffskontrolle, überprüfbaren Nachweisen und interoperablem Datenaustausch. Die regulatorischen Anforderungen bleiben jedoch kumulativ und abhängig vom jeweiligen Anwendungsfall, Sektor und der Rolle des beteiligten Akteurs.

Quellenbasis: Kapitel 2, Annex A und die im Dokument aufgeführten Gaia-X-Quellen [10] bis [16]. Die Zuordnung ist eine analytische Synthese, keine verbindliche Auslegung der Rechtsakte.

gaia-x
Hub Austria

Bleiben wir in Verbindung

Der Gaia-X Hub Austria verbindet Wirtschaft, Forschung und öffentliche Verwaltung rund um ein gemeinsames Ziel: Daten austauschen und nutzen, ohne die Kontrolle über sie abzugeben.

Scannen Sie den QR-Code und folgen Sie dem Gaia-X Hub Austria auf LinkedIn für Neuigkeiten, Veranstaltungen und Einblicke.

Gaia-X Hub Austria
Der Austrian Hub wird betrieben von AIT Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Wien, Österreich
info@gaia-x.at www.gaia-x.at