gaia-x
Hub Austria

GAIA-X HUB AUSTRIA

European Legal Framework for Trustworthy Data Spaces and Gaia-X

Regulatory context and technical relevance

Gaia-X Summit 2026
Vienna, 19 and 20 November 2026



About this position paper

Regulatory context and technical relevance

This position paper examines the regulatory framework for developing and operating trustworthy, interoperable and sovereign data spaces in Europe and analyses its significance for Gaia-X. It focuses on eight key European legal acts: the General Data Protection Regulation (GDPR), the Data Governance Act, the Data Act, eIDAS 2.0, NIS2, the Cyber Resilience Act, the AI Act and the Interoperable Europe Act.

Based on structured, AI-supported research and preliminary assessment, the paper systematically sets out the objectives, relevant stakeholders and key requirements of each legal act and assesses their relevance for Gaia-X and the Austrian data space context. Particular emphasis is placed on linking regulatory requirements with technical and organisational Gaia-X building blocks, especially in the areas of trust, identity management, data sovereignty, compliance, security and interoperability.

The comparative perspective makes regulatory commonalities, overlaps and potential implementation gaps visible. The position paper thus offers structured orientation for companies, public bodies, research and other stakeholders in the European data ecosystem and shows how Gaia-X can contribute to the practical implementation of regulatory requirements and to the establishment of trustworthy data spaces.

EDITOR

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

CONTACT

Gaia-X Hub Austria
Operated by AIT Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Vienna, Austria
info@gaia-x.at www.gaia-x.at

AUTHORS

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

Position paper

Contents

01	**Introduction**	**4**
1.1	Background and motivation	4
1.2	Objectives and scope	4
1.3	Methodology and scope limitations	5
02	**European Legal Framework for Data Spaces and Gaia-X**	**6**
2.1	General Data Protection Regulation (GDPR)	6
2.2	Data Governance Act	7
2.3	Data Act	8
2.4	eIDAS 2 / European Digital Identity Framework	9
2.5	NIS2	10
2.6	Cyber Resilience Act	11
2.7	AI Act	12
2.8	Interoperable Europe Act	13
03	**Summary Assessment**	**15**
	Sources and Further Reading	**16**
A	**Annex A: Comparative Overview of the European Legal Frameworks**	**17**
B	**Annex B: Common Regulatory Requirements and Gaia-X Building Blocks**	**18**

01

Introduction

1.1 Background and motivation

The increasing digitalisation of business, public administration and society is creating a growing need for secure, trustworthy and interoperable data exchange across organisational, sectoral and national borders. Data is an essential foundation for innovation, competitiveness and new digital services. At the same time, data sovereignty, data protection, cybersecurity and the allocation of legal responsibilities are central challenges for cross-organisational data use. The European Union therefore aims to establish a common European data market in which data can be used under clearly defined legal, organisational and technical conditions.

European data spaces (Common European Data Spaces) play a key role here. They enable the controlled exchange and shared use of data between different stakeholders without these stakeholders having to give up control over their data. Data spaces rely on federated architectures, common standards, interoperable technical components and governance structures. They thereby create the conditions for trustworthy data ecosystems in which companies, public bodies, research institutions and other stakeholders can provide and use data under defined conditions.

Gaia-X supports the development of such federated digital ecosystems through common technical specifications, governance principles and verifiable trust mechanisms. The focus is on digital identities, data sovereignty, transparency, interoperability and machine-readable descriptions and evidence for digital services and data offerings.

Gaia-X is not a legal framework in its own right and does not replace statutory compliance obligations. Rather, its technical and organisational mechanisms can help to implement regulatory requirements in practice within federated data ecosystems.

The European legal framework for data spaces has developed considerably in recent years. The Data Governance Act, the Data Act, the General Data Protection Regulation (GDPR), the AI Act and rules on digital identities, cybersecurity and interoperability have created or specified essential conditions for trustworthy European data exchange. These legal acts address different but closely related aspects of the data economy: data access and lawful use, identification and trustworthiness of the stakeholders involved, security of digital infrastructures and traceability of data-based processes. Sector-specific rules, for example on digital product passports, add further requirements for providing and using data across organisational boundaries.

For the development and operation of European data spaces, this results in a complex interplay of regulatory requirements, technical standards and organisational responsibilities. Individual legal acts cannot always be considered in isolation, as data spaces often touch several regulatory areas at once. At the same time, common technical approaches such as those of Gaia-X make it possible to reuse identity management, access control, data exchange and compliance evidence across different areas of application.

1.2 Objectives and scope

The following chapter provides a structured overview of the most important European legal acts relevant to data spaces and the Gaia-X ecosystem. It considers their objectives, scope, key requirements and impact on technical and organisational data space architectures. Particular emphasis is placed on the interactions with Gaia-X and on the extent to which its specifications and trust mechanisms can support the practical implementation of regulatory requirements. In addition, the significance of each legal act for Austrian stakeholders and for Gaia-X Hub Austria is assessed. Annex A summarises the legal frameworks covered, comparing their objectives, governance models, technical building blocks and regulatory requirements; Annex B maps cross-cutting requirements to the relevant Gaia-X building blocks and points out convergences and interoperability potential.

The aim is to create a shared understanding of the regulatory environment and to show the connections between legal requirements, technical implementation options and

strategic developments in the European data ecosystem. The paper is aimed in particular at decision-makers, data space initiatives, technology providers, companies, public bodies and research institutions. It serves as professional orientation and does not replace a legal review of individual use cases.

1.3 Methodology and scope limitations

The study follows a structured, multi-stage approach that combines the systematic capture of European policy and regulatory initiatives with an assessment focused on Gaia-X. First, the scope and categories of the study are defined: relevant legal acts, policy programmes, standards and initiatives related to trustworthy data exchange and federated data spaces are taken into account. A uniform assessment grid records in particular the objective, the stakeholders concerned, the key requirements and the relevance for Gaia-X.

AI-supported web research is then used to identify relevant initiatives and to create structured short profiles. The information obtained in this way is to be understood as an aid to research and structuring; for robust statements, official EU legal sources, publications by the competent institutions and relevant technical specifications are used as the primary basis. In an AI-supported preliminary assessment, the initiatives captured are prioritised according to their significance for Gaia-X and Austria and their relation to trust, compliance and interoperability. The prioritisation is an aid to orientation and does not replace a professional or legal review.

In the intended procedure, the resulting selection is reviewed by selected experts of the Gaia-X Hub in order to validate the assessment, identify gaps and add further initiatives where appropriate. Finally, the results are grouped by topic and relationships, overlaps and common requirements are worked out. The present focus is on eight particularly relevant European legal acts. The uniform “snapshots” in Chapter 2 condense their objectives, addressees, core requirements and Gaia-X relevance; Annex A compares the legal acts, while Annex B maps common requirements to technical Gaia-X building blocks.

The publication thus provides regulatory and technical orientation for the Gaia-X ecosystem in Austria. It claims neither to capture all relevant initiatives completely nor to provide a binding legal interpretation or conformity assessment of individual solutions.

02

European Legal Framework for Data Spaces and Gaia-X

Building on this context, the following sections present the key European legal acts that shape the development, operation and use of trustworthy data spaces. The presentation follows their different regulatory priorities, from the protection of personal data and the conditions for data access, through digital identities, cybersecurity and artificial intelligence, to product information, interoperability and resilience. For each legal act, the key obligations and technical implications are outlined, together with the possible contributions of Gaia-X and the significance for Austrian stakeholders. The chapter closes with an overall view of how these rules interact. Figure 1 shows the thematic classification of the legal frameworks covered and their common reference points for cross-organisational data exchange.

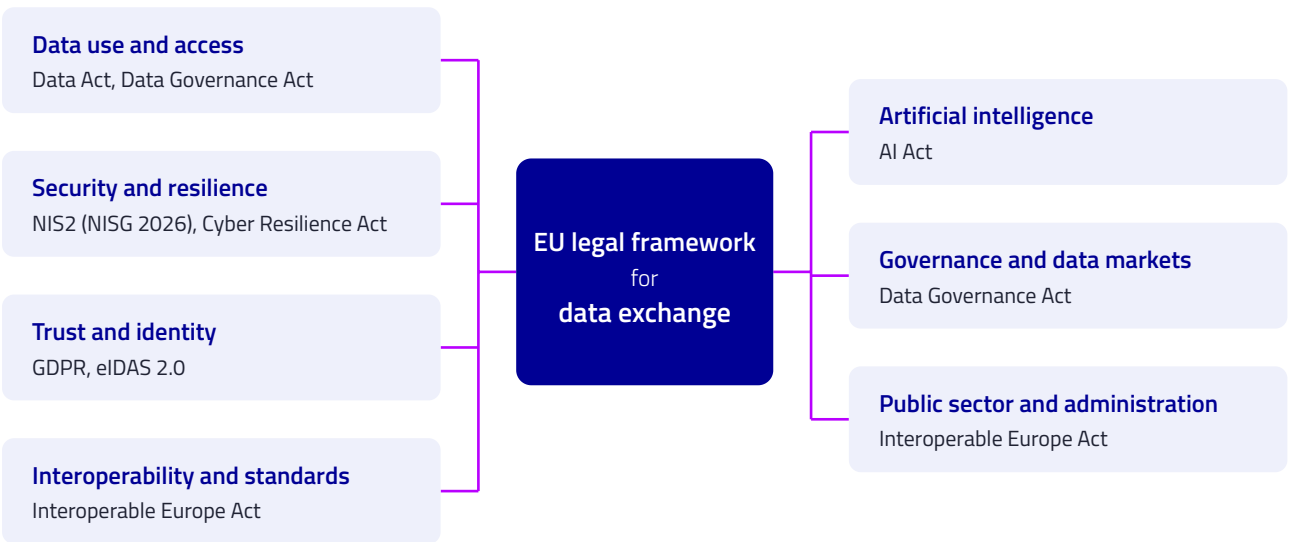


Figure 1 Overview of the relevant EU legal frameworks and their thematic classification.

2.1 General Data Protection Regulation (GDPR)

SNAPSHOT

OBJECTIVE	ADDRESSEES	CORE REQUIREMENTS	GAIA-X RELEVANCE
Protection of personal data	Controllers Processors Data space operators	Legal basis Purpose limitation Security Data subject rights	Identities Access control Policies Evidence

The General Data Protection Regulation (EU) 2016/679 creates a uniform European legal framework for protecting natural persons with regard to the processing of personal data and, at the same time, for the free movement of personal data within the EU. The GDPR generally applies to the automated processing of personal data by private and public organisations. This includes personal data that is provided, analysed or further processed across organisations within data spaces. In Austria, the GDPR is supplemented in particular by the Data Protection Act (Datenschutzgesetz, DSG). Key requirements are lawfulness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. In addition, there are requirements for

privacy by design and privacy by default, data security, data subject rights and, where applicable, data protection impact assessments.[1]

For any specific data exchange, the legal basis under Article 6 GDPR must be determined in particular. Article 28 applies to processing on behalf of a controller, Article 32 to technical and organisational safeguards and Chapter V to transfers to third countries. In networked data ecosystems, distinguishing between personal and non-personal data can be difficult. Gaia-X criteria for cloud services can record information on sub-processors, processing locations and security measures in a comparable form; nevertheless, the review of legal basis, purpose limitation and third-country transfers remains a separate obligation.[1, 16, 21]

STAKEHOLDERS

The stakeholders concerned include controllers, processors, public administrations, companies, data space operators, data providers and users, and natural persons as data subjects. Data spaces must in particular support fine-grained access control, identity management, purpose and authorisation management, logging and secure data transmission. Technical architectures should avoid unnecessarily duplicating or centralising personal data. The GDPR is particularly relevant for data spaces when personal data is shared. Federated architectures can be advantageous here, because data can remain with its respective holders and access takes place in a controlled manner. The European Data Strategy explicitly links the European data space with high requirements for data protection and data security.[1]

GAIA-X

Gaia-X supports principles such as data sovereignty, verifiable identities, controlled data access and policy-based use. These mechanisms can support the technical implementation of data spaces that comply with data protection law. However, Gaia-X compliance does not automatically mean GDPR compliance. Whether data is personal determines the applicable regime, but in networked environments this often cannot be answered clearly. For sub-processors, processing locations and safeguards in place, there is no standardised, verifiable evidence that contractual partners can use without an individual audit. The Gaia-X cloud criteria record information on processing on behalf of a controller and on sub-processors, as well as on processing locations and security measures. Evidence can be provided in a common format and checked according to the respective criterion. The data exchange criteria link usage agreements with authorisations and recipient attributes. This supports the selection of service providers and the documentation of processing. The legal basis, purpose limitation and admissibility of a third-country transfer must be checked in each specific case; Gaia-X evidence does not replace this review.[1, 16, 21]

For Austrian Gaia-X and data space projects, the GDPR is a central cross-cutting requirement. It is particularly relevant for public administration, healthcare, mobility, energy, smart cities and research. Gaia-X Hub Austria can provide orientation here, in particular on combining data protection requirements with federated data architectures.[1, 16, 21]

2.2 Data Governance Act

SNAPSHOT

OBJECTIVE	ADDRESSEES	CORE REQUIREMENTS	GAIA-X RELEVANCE
Trust in voluntary data sharing	Public bodies Data intermediaries Data altruism	Neutral intermediation Registration Secure re-use	Identities Trust Data catalogues Compliance

The Data Governance Act (DGA), Regulation (EU) 2022/868, is intended to increase the availability of data and strengthen trust in voluntary data sharing. In particular, it creates a framework for the re-use of certain protected public sector data, data intermediation services and data altruism. The DGA concerns public bodies, data intermediation services, data altruism organisations and companies and individuals who provide or use data through such mechanisms. This includes neutrality and transparency requirements for data intermediation ser-

vices, protection requirements for the re-use of sensitive public sector data and organisational and legal requirements for data altruism.[2]

The DGA does not itself establish general rights of access to data. Rather, it mainly regulates the role of neutral data intermediation services and their registration and supervision. A practical challenge is that the legally required neutrality is not demonstrated by any uniform technical evidence. Gaia-X can provide verifiable organisational identities and standardised service descriptions for this purpose. Official registrations or evidence of neutrality could be integrated through additional, specifically defined rules for issuers and verification; such an extension does not replace the official procedures.[2, 18, 19, 22]

STAKEHOLDERS

The stakeholders concerned include public authorities, companies, data intermediaries, research institutions, non-profit organisations, data space operators and data holders. Secure data exchange mechanisms, identity and authorisation management, traceable data flows and, where necessary, secure processing environments are required. The DGA is a central regulatory foundation for European data spaces. The existing Gaia-X position paper explicitly names the DGA and the Data Act as important legal acts whose requirements can be implemented or supported particularly well through data spaces.[2, 18, 19, 22]

GAIA-X

Gaia-X complements the DGA technologically and organisationally. While the DGA defines the legal framework for trustworthy data intermediation, Gaia-X can provide identity, trust, catalogue and compliance mechanisms. Applicable since 24.09.2023. Neutrality and trustworthiness are set out in law and are subject to official supervision. A technical proof that would allow market participants to recognise compliance without their own review is not provided for.[2, 18, 19, 22]

Gaia-X offers verifiable organisational identities and a common format for information on services and their conditions. This allows participants and data intermediaries to be checked according to uniform rules when they join a data space. Supplementary rules of a data ecosystem could integrate official registrations or evidence of neutrality, provided that suitable issuers and verification procedures are defined. Such an extension must be set up separately; notification and official supervision under the Data Governance Act remain necessary. For Austria, the DGA is particularly relevant when building sectoral and public data spaces and for potential data intermediaries. Gaia-X Hub Austria can help Austrian organisations to connect DGA requirements with European data space architectures.[2, 18, 19, 22]

2.3 Data Act

SNAPSHOT

OBJECTIVE	ADDRESSEES	CORE REQUIREMENTS	GAIA-X RELEVANCE
Fair data access and data use	Manufacturers Data holders Users Cloud services	Access Sharing Portability Interoperability	Data catalogues Policies Evidence Trust

The Data Act, Regulation (EU) 2023/2854, creates harmonised rules on fair access to and use of data. It focuses in particular on data generated by connected products and related services. It affects manufacturers of connected products, providers of related services, data holders, users, data recipients, public bodies and providers of data processing services. The Data Act gives users rights to access product and usage data and to share it with third parties, sets rules for B2B and B2G data sharing, protects against unfair contractual terms and lays down requirements for switching between cloud and data processing services and for interoperability.[3]

For data spaces, Chapters II to V on access to and sharing of data, Chapter VI on switching between data processing services and Chapter VIII on interoperability are particularly relevant; Chapter VII deals with unlawful governmental access to non-personal data from third countries. Article 33 sets out requirements for the interoperability of common European data spaces. The Data Act has largely

applied since 12 September 2025; Article 3(1) concerns connected products placed on the market from 12 September 2026, while switching charges under Article 29 are to be abolished from 12 January 2027. To specify the interoperability requirements, the Commission published a standardisation request (C(2025) 4135 final) on 1 July 2025. Until relevant harmonised standards are available, uncertainties remain regarding description and evidence formats. Machine-readable Gaia-X service descriptions, terms of use and evidence can support implementation, but on their own do not guarantee full Data Act compliance.[3, 17, 20]

STAKEHOLDERS

Those affected include in particular industrial companies, IoT manufacturers, cloud providers, platforms, public bodies, SMEs, consumers and providers and operators of data spaces. Data increasingly has to be provided in structured and machine-readable formats. APIs, interoperability mechanisms, data catalogues, access control, contract and policy management and portability are becoming considerably more important. Data spaces offer a possible technical infrastructure for putting the Data Act into practice. The available Gaia-X documents show that data spaces can support in particular data access, B2B and B2G data sharing, provider switching and interoperability.[3, 17, 20]

GAIA-X

There is a particularly close link to Gaia-X here: the architecture can provide verified identities, trust, catalogues and compliance mechanisms and thereby support controlled and traceable exchange in line with Data Act principles. The underlying materials describe Gaia-X-based trust frameworks and verified sovereign identities as an important approach for secure exchange relationships. In force since 11.01.2024 and largely applicable since 12.09.2025. Art. 3(1) applies to connected products placed on the market from 12.09.2026. Switching charges are reduced in stages and will be abolished completely from 12.01.2027 (Art. 29). The requirements are worded in abstract terms. The specifications and harmonised standards that would make them concrete are not yet available. Access, portability and interoperability are therefore owed without a binding format for descriptions and evidence. Anyone building today is doing so in advance and must expect adaptation effort once standardisation is available.[3, 17, 20]

Gaia-X describes data offerings and their providers in a common, machine-readable format. The data exchange rules link terms of use with proof of authorisation and documented acceptance of contracts. Cloud criteria require transparency about switching and porting procedures. This enables organisations to compare offerings and reuse evidence. This supports the implementation of access rights and interoperability requirements; fulfilling them completely also requires suitable interfaces, data models and contractual arrangements. Gaia-X compliance is not proof of full Data Act compliance. The Data Act affects numerous Austrian companies in industry, energy, mobility and IoT. For Gaia-X Hub Austria, this opens up a field of activity in particular around Data Act compliant data spaces and interoperable data and cloud services.[3, 17, 20]

2.4 eIDAS 2 / European Digital Identity Framework

SNAPSHOT

OBJECTIVE	ADDRESSEES	CORE REQUIREMENTS	GAIA-X RELEVANCE
Trustworthy digital identities across the EU	Member States Trust services Regulated bodies	EUDI wallets Proof of identity Attestations of attributes	Verifiable credentials Identity Trust

Regulation (EU) 2024/1183 extends eIDAS and establishes a European framework for digital identities, including the European Digital Identity Wallet. The aim is secure and trustworthy digital identification that can be used throughout the EU for public and private services. The framework concerns natural and legal persons, public administrations, trust service providers and private services that use digital identities or electronic attributes. Interoperable wallets, electronic identification, qualified trust services and the issuance and use of electronic attributes and credentials are relevant.[4, 18, 19, 22]

The European digital identity infrastructure is intended in particular to enable electronic proof of identity and attestations of attributes. According to the timetable described in the underlying review, Member States are to provide at least one European digital identity wallet by the end of 2026; acceptance obligations for certain private bodies will follow later. Gaia-X adds machine-readable, digitally signed information on organisations and services to such identity credentials and uses, among other things, verifiable credentials and OpenID-based exchange mechanisms. However, a Gaia-X credential is not automatically a qualified electronic attestation of attributes within the meaning of eIDAS; this requires suitable issuers, technical profiles and the respective legal conditions.[4, 18, 19, 22]

STAKEHOLDERS

Relevant stakeholders include citizens, companies, public administration, identity providers, trust service providers, data space operators and providers of digital services. Verifiable credentials, wallet infrastructures, authentication, credential presentation and interoperability between different identity systems are becoming more important. Data spaces need reliable mechanisms to identify participants and to verify roles, attributes and authorisations. eIDAS 2 can provide an identity layer recognised throughout Europe for this purpose.[4, 18, 19, 22]

GAIA-X

Identity and trust are core components of the Gaia-X model. A central strategic interface therefore exists between European Digital Identity Wallets, electronic attributes and Gaia-X credentials. Gaia-X can build on such regulated identity and trust services and extend them for B2B data ecosystems. The framework is geared towards proof of identity of natural and legal persons. For organisation-related attributes that a data space needs, such as role, certification status or processing location, there is as yet no established system of issuers. The proposal for a European business wallet has not yet been adopted. Gaia-X adds machine-readable, digitally signed information on organisations and services to proof of identity. Its trust model takes account of eIDAS trust service providers and defined sources for verifying organisational data. The specifications use verifiable credentials and OpenID protocols for their exchange. This allows identities to be linked with additional attributes. Trusted issuers must be defined for such attributes. A Gaia-X credential is not automatically a qualified attestation of attributes; connecting to EUDI wallets requires the respective technical profiles and legal conditions.[4, 18, 19, 22]

Austria already has a well-developed national e-ID infrastructure. Austrian Gaia-X ecosystems therefore have particular potential to connect national digital identities with European wallet, trust and data space mechanisms.[4, 18, 19, 22]

2.5 NIS2

SNAPSHOT

OBJECTIVE	ADDRESSEES	CORE REQUIREMENTS	GAIA-X RELEVANCE
High common level of cybersecurity	Essential and important entities IT service providers	Risk management Supply chain security Reporting	Trust Security evidence Transparency

The NIS2 Directive (EU) 2022/2555 aims to create a high common level of cybersecurity across the EU and significantly widens the range of organisations subject to obligations. NIS2 covers many essential and important entities, for example in energy, transport, health, digital infrastructure, public administration, manufacturing and other sectors. Organisations must establish cybersecurity risk management, implement security measures, address supply chain risks, report significant incidents and anchor responsibility at management level.[5]

In the Austrian context, the national transposition of the NIS2 requirements needs particular attention. The regulatory overview used refers to the NISG 2026 (Federal Law Gazette BGBl. I No. 94/2025) and its entry into force on 1 October 2026. Particular emphasis is placed on supply chain security: smaller providers can also be indirectly affected if obliged clients demand corresponding evidence. Standardised information on security audits, for example based on ISO/IEC 27001 or BSI C5, can make repeated bi-

lateral audits easier. However, it replaces neither an organisation's own risk assessment nor safeguards, registrations or statutory reports.[5]

STAKEHOLDERS

The stakeholders concerned include operators of critical and important services, cloud and data centre providers, managed service providers, public bodies and numerous industrial companies. Requirements include security monitoring, incident management, access control, business continuity, supply chain security and documented security measures. Data spaces connect organisations and systems across institutional boundaries. Secure identities, secure interfaces, trustworthy participants and supply chain security therefore become central prerequisites.[5]

GAIA-X

Gaia-X can support NIS2 by making the attributes of participants and services transparent and verifiable. Compliance evidence and trust mechanisms can help to demonstrate security requirements in federated ecosystems; however, Gaia-X does not replace NIS2 risk management. Promulgated on 23.12.2025 as BGBl. I No. 94/2025 and in force from 01.10.2026. Registration must take place within three months of entry into force. A uniform proof with which a supplier can demonstrate its security status to several clients is not provided for. Evidence is provided bilaterally through questionnaires and audits, which creates considerable effort when there are many contractual partners.[5, 16, 21]

Gaia-X can make it easier to assess service providers in the supply chain. Its cloud criteria relate security requirements to existing audit standards, such as ISO/IEC 27001 or BSI C5. Where the respective criterion accepts it, existing evidence can be included in the Gaia-X assessment and used towards several clients. The subject and scope of the audit must remain identifiable. This does not result in full NISG compliance: an organisation's own risk assessment, the implementation of the necessary safeguards and the statutory reporting obligations must be fulfilled separately. NIS2 is particularly relevant for Austrian operators of critical and important services. The previous Austrian NISG is replaced by the NIS2 transposition; the Austrian legal information system (RIS) shows the previous NISG as expiring on 30 September 2026. For Gaia-X Austria, energy, transport, public administration and digital infrastructure are therefore particularly relevant target areas.[5, 16, 21]

2.6 Cyber Resilience Act

SNAPSHOT

OBJECTIVE	ADDRESSEES	CORE REQUIREMENTS	GAIA-X RELEVANCE
Secure products with digital elements	Manufacturers Importers Distributors Software providers	Secure development Vulnerability management Evidence	Machine-readable security attributes Trust

The Cyber Resilience Act, Regulation (EU) 2024/2847, lays down horizontal cybersecurity requirements for products with digital elements and is intended to ensure that hardware and software products are adequately protected throughout their life cycle. It generally covers products with digital elements, including hardware and software, made available on the EU market. Security by design, secure default configurations, vulnerability handling, security updates, technical documentation and reporting obligations are among the central elements.[6]

The CRA provides for staggered application dates: according to the regulatory overview used, reporting obligations under Article 14 apply from 11 September 2026, and the full product requirements including conformity assessment and CE marking from 11 December 2027. The requirements for vulnerability handling include a software bill of materials (SBOM), which documents the components of a product in a commonly used machine-readable format. Federated data spaces can be useful for exchanging such evidence across organisations. Gaia-X could link product versions, signed evidence and references to SBOMs; it does not, however, provide its own SBOM format or a CRA conformity procedure.[7, 15, 17]

STAKEHOLDERS

The stakeholders concerned include manufacturers, importers, distributors, software providers and operators and users of digital products. The secure development lifecycle, vulnerability management, software update processes, documentation and evidence must be systematised. Connectors, software components, IoT devices and other products can be part of a data space ecosystem. CRA compliance therefore increases the security of the technical basis of data spaces.[6]

GAIA-X

Gaia-X could represent CRA-related conformity or security attributes of a product or service as machine-readable trust information. This creates a link between product security and the Gaia-X-based assessment of trustworthy digital resources. In force since 10.12.2024. The reporting obligations under Art. 14 for actively exploited vulnerabilities and severe security incidents apply from 11.09.2026, with an early warning within 24 hours, a notification within 72 hours and a final report within 14 days. From 11.12.2027 the full product requirements apply, including conformity assessment and CE marking. The format and exchange route of the SBOM along the supply chain are not conclusively specified. For further product and component attributes that customers need, there is no uniform verifiable representation.[7, 15, 17]

Gaia-X can support a regulated exchange of software bills of materials and product evidence between identified supply chain partners. The data exchange mechanisms for agreeing terms of use and authorisations can be used for this. A CRA-related extension could link product versions with signed evidence and references to SBOMs. Corresponding data models, issuers and verification rules would have to be defined for this. Gaia-X does not provide its own SBOM format or a CRA conformity procedure; product testing, vulnerability management and reports to authorities remain separate tasks. The CRA is particularly relevant for Austrian software, IoT, automation and industrial companies. For Gaia-X Austria, this points to a possible field of action around digital compliance credentials and automated evidence.[7, 15, 17]

2.7 AI Act

SNAPSHOT

OBJECTIVE	ADDRESSEES	CORE REQUIREMENTS	GAIA-X RELEVANCE
Safe and trustworthy AI systems	AI providers Deployers Data providers	Data governance Documentation Record-keeping	Data provenance Usage rights Trust Evidence

The AI Act, Regulation (EU) 2024/1689, creates harmonised rules for artificial intelligence and is intended to promote safe and trustworthy AI systems while protecting health, safety and fundamental rights. The AI Act covers providers, deployers and other actors along the AI value chain. The regulatory requirements depend on the type and risk of the respective AI system. For regulated systems, risk management, data governance, technical documentation, logging, transparency, human oversight, robustness and cybersecurity may be required in particular.[7]

For data exchange, Article 10 on data governance, Article 11 on technical documentation, Article 12 on record-keeping, Article 25 on the allocation of obligations along the value chain and Article 53 on general-purpose AI models are particularly relevant. According to the underlying review, requirements on AI literacy and certain prohibitions have applied since 2 February 2025, and obligations for general-purpose AI models since 2 August 2025. The overview used also takes account of Regulation (EU) 2026/1744 and names 2 December 2027 for stand-alone high-risk systems under Annex III. The origin and permitted use of training data can be supported by verifiable data product descriptions and transaction records. An assessment of whether data is suitable, as well as the AI-specific documentation and risk management obligations, remain independent of this.[7]

STAKEHOLDERS

Those affected include AI providers, deployers, data providers, research institutions, public bodies and cloud and computing providers. Data provenance, data quality, documentation, logging, model governance and traceable

AI pipelines are becoming more important. Data spaces can provide trustworthy and controllable data sources for AI. They also enable the cross-organisational use of training, validation and operational data under defined conditions.[7]

GAIA-X

A Gaia-X synergies paper describes AI as a particularly suitable field of application for the Gaia-X Trust Framework: high-quality data, algorithms and computing resources can be provided through federated trustworthy ecosystems. In force since 01.08.2024. Prohibited practices and the requirements on AI literacy have applied since 02.02.2025, and the obligations for general-purpose AI models since 02.08.2025. The Digital Omnibus Regulation on artificial intelligence, Regulation (EU) 2026/1744, was published on 24.07.2026 and has been in force since 27.07.2026. Stand-alone high-risk systems under Annex III are subject to the obligations from 02.12.2027. The regulation requires documentation, but does not prescribe a format for cross-provider proof of origin. The lack of finished harmonised standards under Art. 40 was one of the reasons for postponing the deadlines for high-risk systems.[8, 17, 20]

Gaia-X can support the sourcing of data for AI applications: descriptions of data products link providers and usage rights with verifiable evidence. The data exchange specifications take account of transaction logging. This can produce evidence of the origin and permitted use of the data obtained. AI-specific quality criteria would require additional rules and verification procedures. The suitability of a dataset for a specific AI system and the fulfilment of documentation and risk management obligations must be assessed separately. Austria has strong industrial AI, research and public sector ecosystems. Gaia-X Austria can address in particular trustworthy AI data spaces, data provenance and access to federated computing resources. [8, 17, 20]

2.8 Interoperable Europe Act

SNAPSHOT

OBJECTIVE	ADDRESSEES	CORE REQUIREMENTS	GAIA-X RELEVANCE
Cross-border interoperability in the public sector	Authorities EU institutions Public IT services	Interoperability assessments Common solutions	Federation Service descriptions Trust

The Interoperable Europe Act, Regulation (EU) 2024/903, aims to achieve a high level of cross-border interoperability in the EU public sector. It concerns EU institutions and public bodies of the Member States, in particular for cross-border digital public services. Key elements are interoperability assessments, joint governance, the reuse of interoperable solutions and support for common European solutions.[8]

For public digital services with cross-border relevance, interoperability assessments may be required before network and information systems are introduced or significantly changed. Uniform service descriptions and verifiable attributes, as supported by Gaia-X, can make comparison and documentation easier. The statutory assessment and the alignment of domain data models and organisational responsibilities must be carried out by the competent public bodies themselves.[11, 18, 19, 22]

STAKEHOLDERS

This concerns ministries, authorities, federal states, municipalities, EU institutions and public IT service providers. Open interfaces, common data models and reusable components strengthen technical, semantic and organisational interoperability.[8]

GAIA-X

Gaia-X can complement trust and federation between public and private participants. Applications in which public data is combined with company data or research data are particularly interesting. The assessment requires systems that can be described and comparable description formats. The legal act specifies neither. Gaia-X offers common description models for organisations and digital services as well as verifiable information on their conditions. Public bodies can use this information to compare offerings and to document cross-organisational data exchange relationships. The contribution lies above all in technical and semantic agreement on identities and evi-

dence. This information can support an interoperability assessment. The legally required assessment and the alignment of domain data models and of legal and organisational prerequisites remain the tasks of the public bodies involved.[11, 18, 19, 22]

The Act is relevant for the federal government, the federal states and municipalities and fits directly with Austrian smart city, administrative and municipal data space activities. For Gaia-X Austria, this is therefore a strategically relevant public sector topic.[11, 18, 19, 22]

03

Summary Assessment

The eight legal acts presented in Chapter 2 do not form a single legal framework for data spaces; rather, they complement each other in their requirements on data protection, data access, governance, identity, cybersecurity, AI and interoperability. This results in technical and organisational points of contact for Gaia-X, without Gaia-X compliance replacing the fulfilment of individual statutory obligations.

For Gaia-X, the strategic significance lies above all in providing reusable trust and interoperability mechanisms. Verifiable organisational identities, machine-readable descriptions of data offerings and digital services, traceable terms of use and defined procedures for assessing evidence can make exchange easier between stakeholders who have so far been separate. Such common building blocks can be used across sectors and use cases and supplemented with the specific requirements of a data ecosystem. However, technical support from Gaia-X must be clearly distinguished from the legal fulfilment of individual obligations: Gaia-X evidence or the fulfilment of certain criteria does not in itself establish full compliance with the GDPR, the Data Act, NIS2 or other legal acts.[15, 16, 17, 18, 19, 22]

Practical implementation should therefore start from the roles and data exchange relationships. An organisation can at the same time be a data holder, a data user, the operator of a data space, the provider of a data processing service or the deployer of an AI system. For each of these roles, the relevant rights, obligations and contractual relationships must be clarified. Three questions provide an overarching starting point: Who is the counterpart and how are its attributes proven? In what form can data be exchanged in a technically and semantically interoperable way? Under which legal, contractual and organisational conditions is the use permitted? The answers determine which identity, policy, interface and evidence mechanisms are actually needed.[2, 3, 8, 23]

Evidence is a particular field of action. Several legal acts require documented security measures, data provenance, usage rights or compliance with certain procedures without specifying a uniform technical format for all cross-organisational evidence. Gaia-X can support the structured provision and verification of defined attributes here and integrate existing certifications or declarations into interoperable trust processes. However, which evidence is accepted, who may issue it and how its validity is checked must be defined for the respective use case. Legal reviews of individual cases, official procedures and the responsibility of the organisations involved also remain in place.[16, 17, 21]

For Gaia-X Hub Austria, this results in a mediating and coordinating role between European regulation, technical specifications and Austrian data space initiatives. A strategic focus can be to translate regulatory requirements into concrete technical and organisational requirements, to make reusable trust and compliance building blocks visible and to promote cross-sector synergies. Industrial supply chains and digital product passports, energy and mobility data spaces, public and municipal data ecosystems and use cases around critical infrastructures and trustworthy AI offer particularly good starting points. Existing national infrastructures and European standards should be taken into account to avoid parallel isolated solutions.[15, 18, 19, 22]

For the further development of an Austrian Policy & Initiative Radar, this results in an ongoing task of monitoring and translation. In addition to the status and application dates of the legal acts, implementing acts, harmonised standards, technical specifications and new evidence procedures are particularly relevant. Such a radar can make changes visible at an early stage, assess their impact on specific data space roles and architectures and derive prioritised fields of action for Austrian stakeholders. The added value of Gaia-X therefore lies not in a blanket promise of compliance, but in practically supporting trustworthy and interoperable data exchange under evolving regulatory conditions.[15, 20, 23]

Sources and Further Reading

The following selection comprises the EU legal acts covered in this paper and the Gaia-X documents cited in the underlying materials. Legal acts can be found on EUR-Lex by their official number. The links to Gaia-X specifications refer to the documentation pages cited in the review.

[1] European Union (2016): General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

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

[3] European Union (2023): Data Act, Regulation (EU) 2023/2854.

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

[5] European Union (2022): NIS2 Directive, Directive (EU) 2022/2555.

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

[7] European Union (2024): Artificial Intelligence Act, Regulation (EU) 2024/1689; amendment cited in the review: Regulation (EU) 2026/1744.

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

[9] Gaia-X AISBL (2025): Gaia-X Synergies with prominent European data, cloud and digital policy initiatives & projects, Version 1.0, December 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), review document provided; supplementary editorial basis.

Note: This compilation is based on the documents provided. Currency, application status and individual legal references have not been independently reviewed by legal experts.

Annex A

Comparative Overview of the European Legal Frameworks

The following overview condenses the legal frameworks covered in Chapter 2 by their objectives, governance models, technical building blocks and regulatory requirements. The last column names key convergences, overlaps and interoperability potential. The statements are intended as condensed orientation; the Digital Product Passport is a regulatory instrument and not a legal act in its own right.

Legal framework	Objectives & governance	Technical building blocks	Regulatory requirements	Convergence, overlap & interoperability
2.1 GDPR	Protection of personal data; free movement of data Controllers and processors; data subject rights	Access control; pseudonymisation; logging	Legal basis; purpose limitation; data minimisation; security	Common identity and access layer; applies cumulatively with the Data Act
2.2 Data Governance Act	Trust in voluntary data sharing; re-use of protected public sector data Neutral data intermediaries; registered services; data altruism	Identity verification; authorisations; secure processing environments	Neutrality; transparency; notification and supervision	Trust evidence complements Gaia-X; no access rights of its own
2.3 Data Act	Fair data access; sharing; cloud switching Data holders, users, recipients and cloud providers; B2G exceptions	APIs; data models; portability; catalogues	Access rights; contractual fairness; interoperability; switching obligations	Art. 33 on data space interoperability; complements GDPR/DGA
2.4 eIDAS 2	Trustworthy digital identities and attributes across the EU Member States; wallet providers; trust services	EUDI wallet; verifiable credentials; attestations of attributes	Recognition and acceptance of digital identities; trust services	Identity basis for Gaia-X; Gaia-X credentials not automatically qualified
2.5 NIS2	High common level of cybersecurity Essential and important entities; management responsibility	Monitoring; incident management; access protection; business continuity	Risk management; supply chain security; reporting obligations	Security evidence for participants; complements CRA and CER
2.6 Cyber Resilience Act	Security of products with digital elements Manufacturers; importers; distributors	Secure development; vulnerability management; SBOM; updates	Security by design; documentation; reporting; conformity assessment	SBOM and product evidence exchangeable via data spaces; complementary to NIS2
2.7 AI Act	Safe, trustworthy AI that respects fundamental rights Providers; deployers; actors in the AI value chain	Data provenance; logging; model and data documentation	Risk management; data governance; transparency; oversight	Data spaces support evidence; no automatic AI Act compliance
2.8 Interoperable Europe Act	Cross-border interoperability of public services Public bodies; joint European governance	Open interfaces; semantic models; reusable solutions	Interoperability assessments; cooperation; reuse	Connecting public data spaces to Gaia-X trust mechanisms

Note: The technical building blocks describe possible or obvious implementation mechanisms and are not in every case directly required by law. Gaia-X supports technical evidence but does not replace a conformity assessment specific to each legal act.

Annex B

Common Regulatory Requirements and Gaia-X Building Blocks

The following mapping groups recurring requirements from the European legal frameworks described in Chapter 2 and Annex A and compares them with possible Gaia-X building blocks. It serves as orientation for designing federated data spaces. The Gaia-X mechanisms named support technical and organisational implementation; on their own they establish neither legal compliance nor certification.

Common requirement	Legal frameworks (Ch. 2)	Possible Gaia-X building blocks	Convergence / interoperability	Limits / implementation needs
Identity and authentication	GDPR (2.1) eIDAS 2 (2.4) NIS2 (2.5)	Gaia-X Identity, Credential and Access Management (ICAM) Verifiable identity and organisational credentials	Uniform verification of stakeholders and roles Trust relationships across federations	Identity credentials are not automatically eIDAS-qualified; protection needs and level of assurance depend on the context.
Access rights and data use	GDPR (2.1) Data Act (2.3) DGA (2.2)	ICAM and authorisation Data Exchange Services; machine-readable terms of use	Role- and purpose-bound permissions Enforcement of terms of use at exchange points	Legal bases, statutory access rights and contractual conditions must be reviewed separately.
Transparency and verifiable evidence	DGA (2.2) AI Act (2.7) Data Act (2.3)	Gaia-X Compliance Document Trust Anchors Evidence/attestations and criteria assessment	Traceable statements about services and stakeholders Reusable evidence for partner reviews	Gaia-X compliance does not replace legally required audits or conformity assessments.
Cybersecurity and resilience	NIS2 (2.5) CRA (2.6)	Trustworthy identities and access control Verifiable security attributes of digital services	Common minimum requirements for trustworthy services Exchange of security-related evidence	Incident reporting, product security, operational resilience and certification have different addressees and obligations.
Interoperability and data portability	Data Act (2.3) Interoperable Europe Act (2.8)	Gaia-X Data Exchange Services Common descriptions, interfaces and metadata	Federated data exchange across organisational boundaries Connectivity between different data spaces	Domain data models, sectoral standards and public interoperability rules are still required in addition.
Data provenance and traceability	AI Act (2.7) GDPR (2.1)	Verifiable evidence and descriptions Trust anchors and documented data flows	Verification of origin and responsibilities Reusable chains of evidence	Product passport, AI and data protection obligations each require their own domain content and documentation.
Governance and allocation of roles	DGA (2.2) GDPR (2.1) Interoperable Europe Act (2.8)	Gaia-X compliance criteria Descriptions of roles, participants and services	Transparent responsibilities in federated ecosystems Common onboarding rules	Statutory roles (e.g. controller, data intermediation service) are not replaced by Gaia-X roles.

Common requirement	Legal frameworks (Ch. 2)	Possible Gaia-X building blocks	Convergence / interoperability	Limits / implementation needs
Trustworthy digital services	eIDAS 2 (2.4) NIS2 (2.5) CRA (2.6)	Gaia-X Trust Anchors Compliance criteria for digital and cloud services	Uniform verification of service attributes Trust-based cooperation	Gaia-X criteria must be distinguished from formal EU certifications and qualified trust services.

Assessment: There is particularly strong overlap in identity and trust management, access control, verifiable evidence and interoperable data exchange. However, the regulatory requirements remain cumulative and depend on the respective use case, sector and the role of the stakeholder involved.

Source basis: Chapter 2, Annex A and the Gaia-X sources [10] to [16] listed in this document. The mapping is an analytical synthesis, not a binding interpretation of the legal acts.

gaia-x
Hub Austria

Let’s stay connected

Gaia-X Hub Austria connects business, research and public administration around a shared goal: enabling organisations to exchange and use data while retaining control over it.

Scan the QR code and follow Gaia-X Hub Austria on LinkedIn for news, events and insights.

Gaia-X Hub Austria
Operated by AIT Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Vienna, Austria
info@gaia-x.at www.gaia-x.at