Gaia-X MAGAZINE

June 2026 | Edition 8

Familiarise yourself with the latest **Project Updates** p.12

Read the latest **Community Updates** p.52

Learn about Upcoming **Gaia-X Events** p.82

HIGHLIGHT

Gaia-X Season 2.0: Sovereign, Trusted AI & Data Ecosystems

Read our main story on p. 8

TABLE OF CONTENTS

INTERACTIVE

Click on the article title in this overview to go straight to the article page. Happy reading!

01

FOREWORD – WELCOME

Dear readers,

Welcome to the eighth edition of Gaia-X Magazine.

This edition comes at an important moment for our community. Across Europe, we are moving from building the foundations of trusted data spaces to scaling them in practice. That is the essence of Season 2.0: making data spaces operational, economically viable, and capable of delivering real value across sectors and borders.

A good example of this transition is the second phase of the Data Spaces Support Centre, which now focuses on adoption, sustainability, and broader impact. This reflects the wider direction of our ecosystem: from pilots and frameworks to deployment, interoperability, and long-term use. At the same time, the expansion of the International Advisory Board reflects Gaia-X's growing global relevance and the rising demand for trusted, interoperable data ecosystems beyond Europe.

The stories in this edition show that progress clearly. They reflect the work of our Members, Hubs, Lighthouse Projects and partners who are helping turn trust, interoperability, and digital sovereignty into practical realities.

Thank you for your continued commitment to Gaia-X and to the shared vision of a European digital ecosystem built on trust and collaboration.

Warm regards,

Ulrich Ahle
CEO, Gaia-X

That is the essence of Season 2.0: making data spaces operational, economically viable, and capable of delivering real value across sectors and borders.

Ulrich Ahle

02

MAIN STORY
HIGHLIGHTED

In every edition of our magazine, we are thrilled to present you with a highlighted story, offering a comprehensive and captivating exploration of a significant topic. Within this section, you can expect to find engaging interviews with key figures, expert analysis, and the latest updates.

02

2.1

Gaia-X Season 2.0: Sovereign, Trusted AI & Data Ecosystems

Communications Team, Gaia-X

Gaia-X Season 2.0 marks the **transition from technical development to large-scale market adoption of data spaces** in Europe and beyond.

Season 1.0 established the foundation: a unified architecture and essential building blocks that enable trusted data transactions, alongside organisational frameworks that support business, legal, and governance interoperability. **Gaia-X Trust Framework** now enables automated compliance checking, supported by operational **Digital Clearing Houses**.

Progress includes 600+ cloud and edge services in the CISPE catalogue, 14 of which comply with **Gaia-X Label Level 3**, and 200+ use cases across **Gaia-X Lighthouse Ecosystems**. Standards are advancing through CEN/CENELEC and ISO/IEC.

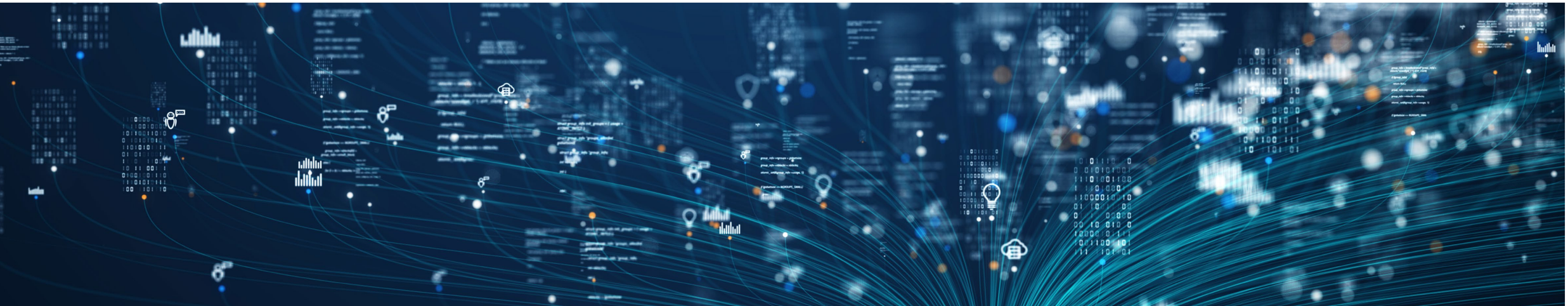
Building on this foundation, Gaia-X officially launched Season 2.0 of Data Spaces and Digital Ecosystems at the Gaia-X Summit in Porto in November 2025. Momentum continued at the Gaia-X European Parliament Reception in Brussels in February 2026, which showcased "Digital Ecosystems in Action". This trajectory was further reinforced at the Governmental Advisory Board meeting in Brussels in April 2026, where priorities were set to accelerate **market adoption** and deliver **tangible economic value**.

Strategic Priorities for Market Adoption

Priorities include establishing **economically sustainable operations for data spaces**, promoting the **adoption of existing technologies**, and enabling the provision of **trustworthy data** for trustworthy **AI** applications.

A strong emphasis is also placed on **simplifying participation for SMEs** and **advancing cross-data-space interoperability** to reduce fragmentation and strengthen strategic data autonomy. **Standardisation** efforts will continue in close collaboration with European and international bodies.

As a result, Gaia-X is moving towards a future where **trust is automated, sovereignty is actionable, and Europe's digital future is built on shared, secure, and transparent foundations**.



01 The Challenge

Data Spaces are **not systems to deploy;**

they are ecosystems to design.

02 The Risk

They fail when **governance and trust are not operationalized and automated.**

03 The Gaia-X Solution

Gaia-X **turns governance and trust into reusable, verifiable capabilities.**

The Gaia-X Trust Framework enables **interoperability & scalability.**

04 The Foundation

Gaia-X: the foundation for scalable digital ecosystems.

Membership determines whether you **consume trust or shape it.**

The Road to Trusted Data Spaces

Data Spaces should not be approached as systems that can simply be deployed; they are ecosystems that must be thoughtfully designed. Their success depends on establishing governance and trust as integral operational capabilities rather than treating them as afterthoughts.

When governance and trust are not effectively operationalised and automated, Data Spaces struggle to scale and often fail to deliver their intended value. Gaia-X addresses this challenge by transforming governance and trust into reusable, verifiable capabilities that organisations can adopt with confidence.

Through the Gaia-X Trust Framework, participants gain a foundation for interoperability, enabling diverse stakeholders to collaborate seamlessly while supporting scalability across digital ecosystems. As a result, Gaia-X provides the foundation for building scalable digital ecosystems, while membership determines whether you consume trust through established frameworks or actively shape it.

As Gaia-X Season 2.0 drives market adoption and delivers tangible economic value in a world where resilient supply chains, digital sovereignty, and cybersecurity have become strategic imperatives, preparations are already underway for the Gaia-X Summit in Vienna in November 2026. The summit will take place under the theme **"Season 2.0: Sovereign, Trusted AI & Data Ecosystems,"** marking the next step in Gaia-X's journey toward a trusted and competitive digital economy.

03

Gaia-X **PROJECT DEVELOPMENTS**

This dedicated section about project developments aims to bring you closer to the forefront of the progress made on the Gaia-X project. It discusses the latest advancements, initiatives, and achievements both from a technical and operational perspective. Whether you are part of the Gaia-X community, an industry professional seeking information or simply an avid reader with a curiosity, this section is for you.

Technology

Operations

Communications

03

3.1.1

CTO Introduction: “TOOLS, TOOLS, TOOLS”

Christoph Strnadl, Chief Technology Officer at Gaia-X

While providing the required software for checking compliance with our compliance document (and any extensions) is, of course, one of the most important tasks of the CTO team, we have been also asked to provide suitable software tools simplifying the process of creating the initial compliance request which then gets sent to one of our compliance engines for conformity checking. The following articles provide a short overview of the most recent additions to our tool suite and a significant improvement of our Gaia-X 3.0 “Danube” Platform towards increased interoperability – not the least with the upcoming EU Business Wallet.

Finally, a note to potential software contributors: If you have a decent tool you want to get listed on our Gaia-X tooling page, just reach out to our CTO. You are also cordially invited to introduce your tool in one of the next Gaia-X Magazines (if you want to) and the OSS Community Call every Thursday, 9:00-9:45 (strongly recommended). Just contact me for that.

3.1.2

From Complexity to Credential:

How the Gaia-X Credential Wizard simplifies obtaining a Participant Compliance Credential under the Loire Trust Framework

Ryan Reychico, Software Engineer at Gaia-X

1. Introducing the Gaia-X Wizard

Obtaining a Participant Compliance Credential by hand means assembling a certificate, a de-centralised identifier, three separate credentials, client-side signing and clearing-house validation — a lot of moving parts for any team. The **Gaia-X Participant Credential Wizard** folds all of that into a single guided interface.

Technically, the Gaia-X Participant Credential Wizard v2.0.0 is a free, browser-based web application. It helps organisations create and sign verifiable presentations and obtain a Gaia-X Participant Credential based on the criteria of the current version (2.5) of the Gaia-X Compliance Document. It is equally useful as a learning tool, making the abstract concepts of verifiable presentations (VP) and verifiable credentials (VC) tangible by letting you build them one step at a time.

It is designed for a broad audience:

- **Organisations** preparing to become Gaia-X participants
- **Compliance and trust managers** who need a defensible, auditable process
- **Technical architects and identity specialists** working with DIDs and credentials
- **Ecosystem federators** guiding members through onboarding

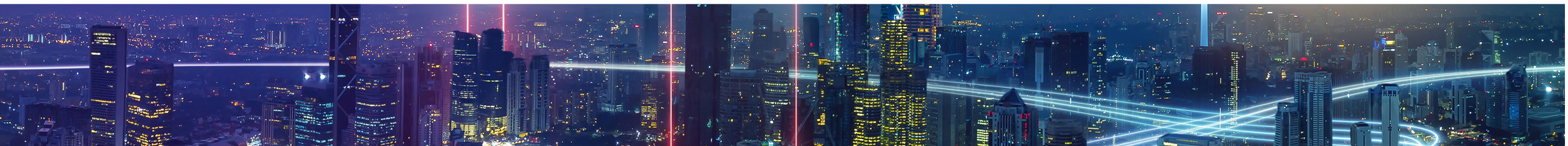
Compared with doing everything by hand, the Wizard adds real value: a visible progress **stepper**, an integrated call to the Gaia-X Registration Number Notary, **client-side signing** that keeps your private key on your own machine, and one-click submission to a Clearing House.

2. Before You Begin: What Production Mode Needs

Because production mode issues credentials under **your own identity**, a few things must be in place before you can productively use the Wizard. Two of them are obtained **outside** the tool, so it is worth preparing them in advance:

What you need	Description
EV-SSL or eIDAS certificate	Issued by a Trust Service Provider recognised as a Gaia-X Trust Anchor. This is requested and obtained outside the Wizard.
did:web DID document	A publicly resolvable decentralised identifier document **(did.json)** linked to that certificate. The Wizard links to a generator if you still need one.
Private key	The key corresponding to your verification method. It is used only inside your browser to sign your credentials and is never sent to a server.
Legal Registration Number	Your organisation's identifier in an accepted format: EORI, VAT ID, or LEI Code.
Credential identifier URLs	Publicly resolvable URLs that will serve as the identifiers for the credentials you create.

With these in place, you are ready to start. In production mode the Wizard automatically submits your Verifiable Presentation to one of the official, certified **Gaia-X Digital Clearing Houses** (GXDCH) — which only accept certificates from recognised Trust Anchors such as eIDAS or EV-SSL — and returns a real, officially recognised Compliance Credential tied to your organisation.



3. The Guided Compliance Journey

The heart of the Wizard is a seven-stage stepper displayed across the top of the screen, so you always know where you are. Each stage gathers one piece of the puzzle and hands off cleanly to the next.

The seven production stages, mirrored by the Wizard's progress bar.

1 Start. A concise overview lays out the full journey, including the two external prerequisites the Wizard cannot perform for you. A single toggle — "I'll use my own private key for signing (production use)" — puts you in production mode for everything that follows.

2 Legal Person. You enter your organisation's legal name, its Legal Registration Number (choosing the type), and the headquarter and legal-address countries. Behind the scenes the Wizard calls the Gaia-X Registration Number Notary to validate the number and return a signed Legal Registration Number credential — so you don't have to craft it yourself.

3 Terms & Conditions. You review and accept the Gaia-X Trust Framework Terms & Conditions with a single checkbox, which generates the corresponding credential recording your acceptance

.

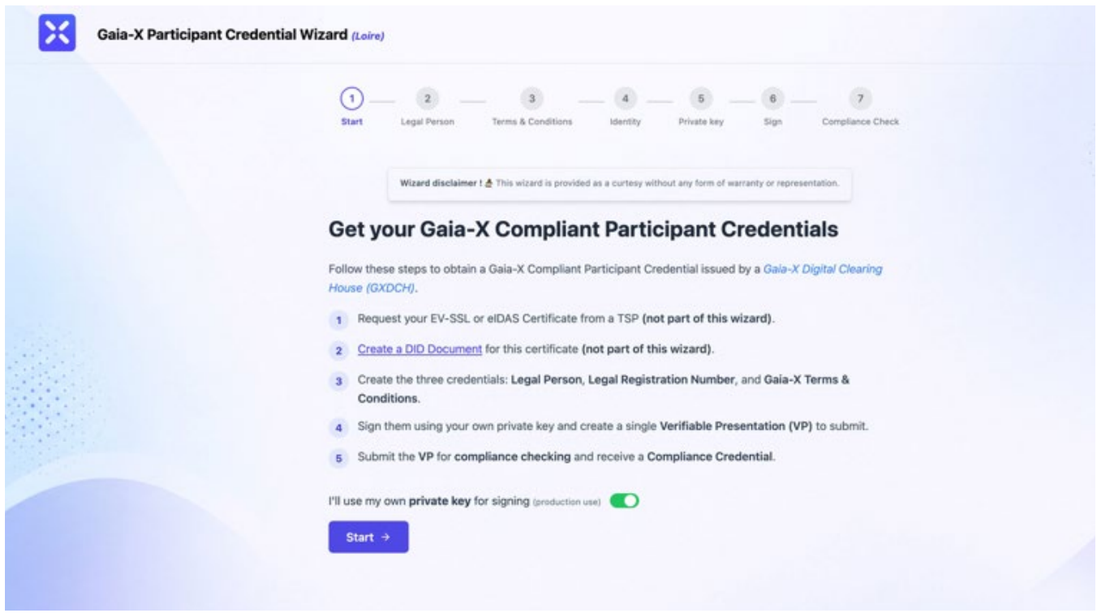


Figure 1. The Start screen: the progress bar, the five-point overview, and the production-mode toggle.

4 Identity. You supply your did:web issuer, the verification method from your DID document (did.json), and the public URLs that will identify each credential. A linked did:web document generator is provided for anyone who still needs one.

5 Private key. You paste your private key. Crucially, it is used purely on your own machine to sign your credentials and is never transmitted to any server — the next section explains exactly how this is handled.

6 Sign. The Wizard signs your credentials and bundles them into a single Verifiable Presentation, ready for submission.

7 Compliance Check. The Verifiable Presentation is sent to a Gaia-X Digital Clearing House. If every credential checks out, the GXDCH returns your signed Compliance Credential, which you can then download together with your other credentials as a single archive.

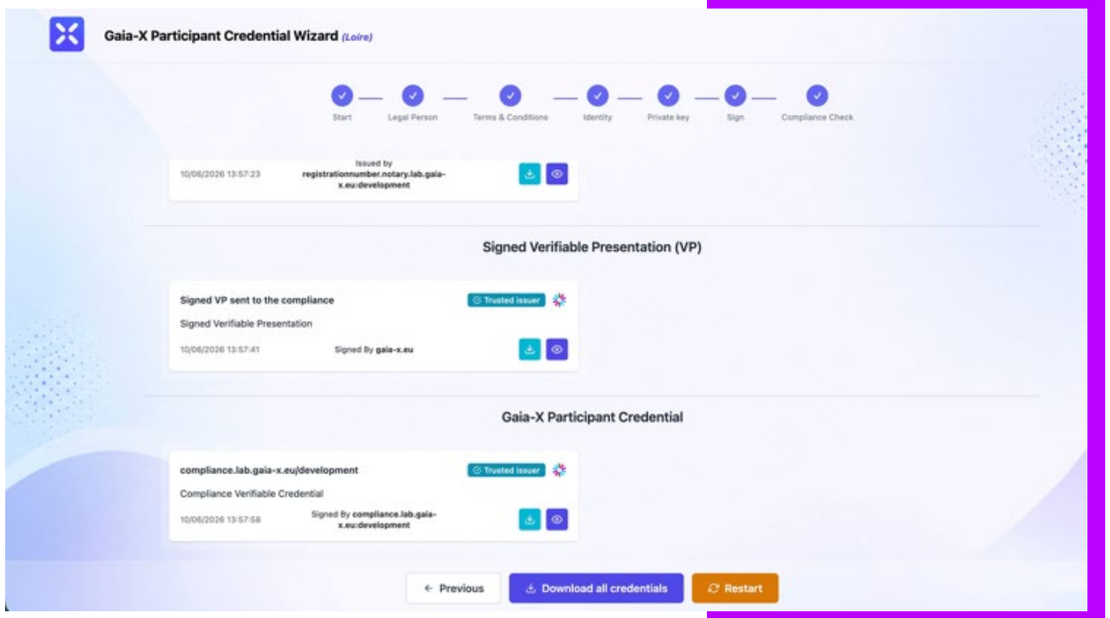


Figure 2. The final screen: the signed Verifiable Presentation and the issued Gaia-X Participant (Compliance) Credential, ready to download.

4. Privacy and Security: Your Key Stays With You

For most organisations the single most sensitive element of the whole process is the **private key** used for signing — and this is precisely where the Wizard is designed to be careful. Although you type your key into the Private key step, the Wizard treats it as something to be used, not stored or shared.

YOUR PRIVATE KEY NEVER LEAVES YOUR BROWSER

- **Never sent over the network**. Signing happens entirely on your machine. The key is not uploaded to the Wizard, to the Clearing House, or to any other server.
- **Never written to storage**. It is held only in memory for the brief moment it is needed — it is not saved to local storage, session storage, cookies, or any other persistent browser store.
- **Used for one purpose only**. It signs your Verifiable Credentials locally, producing the signatures that the Clearing House later verifies against your public DID.

In practice this means the cryptographic material that proves your identity stays under your control at all times. Only the resulting **signed credentials** — never the key itself — travel onward for compliance checking. The same client-side principle runs through the whole tool: the Wizard acts as a guided interface around your own keys and identifiers, not as a custodian of them. For organisations bound by strict data-protection or key-management policies, that distinction matters.

5. The Credentials You Generate

By the end of the flow you hold a small, coherent bundle of credentials — three that you (or the Notary) create as inputs, and one that a Gaia-X Digital Clearing House issues as the result.

Credential	Why it matters
Legal Person verifiable credential (VC)	Describes your organisation as a Gaia-X participant — legal name, headquarter and legal-address countries, and a reference to your registration number. Signed under your own DID.
Legal Registration Number VC	Proves your legal existence via a government-issued identifier (EORI, VAT ID, or LEI Code). It is fetched and signed by the Gaia-X Registration Number Notary, not by you.
Gaia-X Terms & Conditions VC	A self-signed record that you accepted the Gaia-X Trust Framework Terms & Conditions, with a document hash and timestamp.
Gaia-X Participant Credential	The output. Signed by a GXDCH, it references the other three and confirms that your organisation meets the criteria of the current Gaia-X Compliance Document v2.5.0. This credential is your proof for this fact.

6. Key Benefits

- **Simplified onboarding** — one guided interface replaces a chain of disconnected manual tasks.
- **Reduced complexity** — the Notary call, credential assembly and Verifiable Presentation packaging happen for you.
- **A guided, transparent process** — the seven-step stepper keeps your progress visible at all times.
- **Privacy and security by design** — client-side signing keeps your private key on your own machine, never transmitted or stored.
- **Native verifiable-credential support** — built around W3C DIDs and VCs, the standards that underpin Gaia-X trust.
- **Interoperability** — credentials are issued in a form any Gaia-X participant can independently verify.
- **Faster access to the ecosystem** — a clear path from organisation details to a signed Compliance Credential.

USEFUL LINKS

Gaia-X Wizard
wizard.lab.gaia-x.eu
Wizard User Guide
wizard.lab.gaia-x.eu/userGuide
Get a Legal Registration Number
wizard.lab.gaia-x.eu/legalRegistrationNumber
did:web Document Generator
mydid.info
Gaia-X Digital Clearing House (GXDCH)
docs.gaia-x.eu/#/gxdch
Gaia-X Trust Framework documentation
docs.gaia-x.eu
Contribute (source)
gitlab.com/gaia-x/lab/.../gx-signing-tool

7. Conclusion

Gaia-X compliance rests on rigorous cryptographic standards — and that rigour can be intimidating. The Gaia-X Participant Wizard's achievement is to make those standards **approachable** without diluting them. By guiding organisations through each stage of the Loire process, calling the Registration Number Notary on their behalf, signing securely on the user's own machine, and submitting directly to a Digital Clearing House, it turns a daunting technical exercise into a process most teams can complete in a single sitting.

If your organisation is ready to obtain an official Gaia-X Participant Credential, gather your certificate, DID document and registration number, and let the Wizard guide you through the rest: wizard.lab.gaia-x.eu.

3.1.3

From Back-End to Wallet: OID4VP and OID4VCI in the Gaia-X Compliance Dispatcher

Delphine Claerhout, Software Engineer at Gaia-X

An upcoming release of the gx-compliance-dispatcher will add support for OID4VCI and OID4VP v1.0 — meaning Danube compliance credentials will be able to live in your wallet, without the extra fuss.

Overview

Up until now, the Gaia-X Danube Compliance Dispatcher has been a purely back-end affair: it receives a (HTTP/REST) request, routes it to the right extension, and returns a signed response. Works fine but remains quite technical and less interoperable.

That's about to change. The dispatcher will soon be able to ask a wallet directly for the credentials it needs, pass them along to the right extension, and hand the resulting compliance credential back into that same wallet. One conversation, two protocols.

OID4VP (OpenID for Verifiable Presentations) is the "show me your credentials" half - it's how the dispatcher asks the wallet for proof of who the user/organisation is, and how the wallet packages and signs that proof so the dispatcher can verify it came from a genuine, untampered credential.

OID4VCI (OpenID for Verifiable Credential Issuance) is the "here's your new credential" half - it covers how a fresh credential is offered to a wallet, how the wallet authenticates itself (via the pre-authorised code and proof of possession), and how it pulls down and stores the result. In short: OID4VP moves credentials out of the wallet for verification, OID4VCI moves a credential into the wallet for safekeeping.

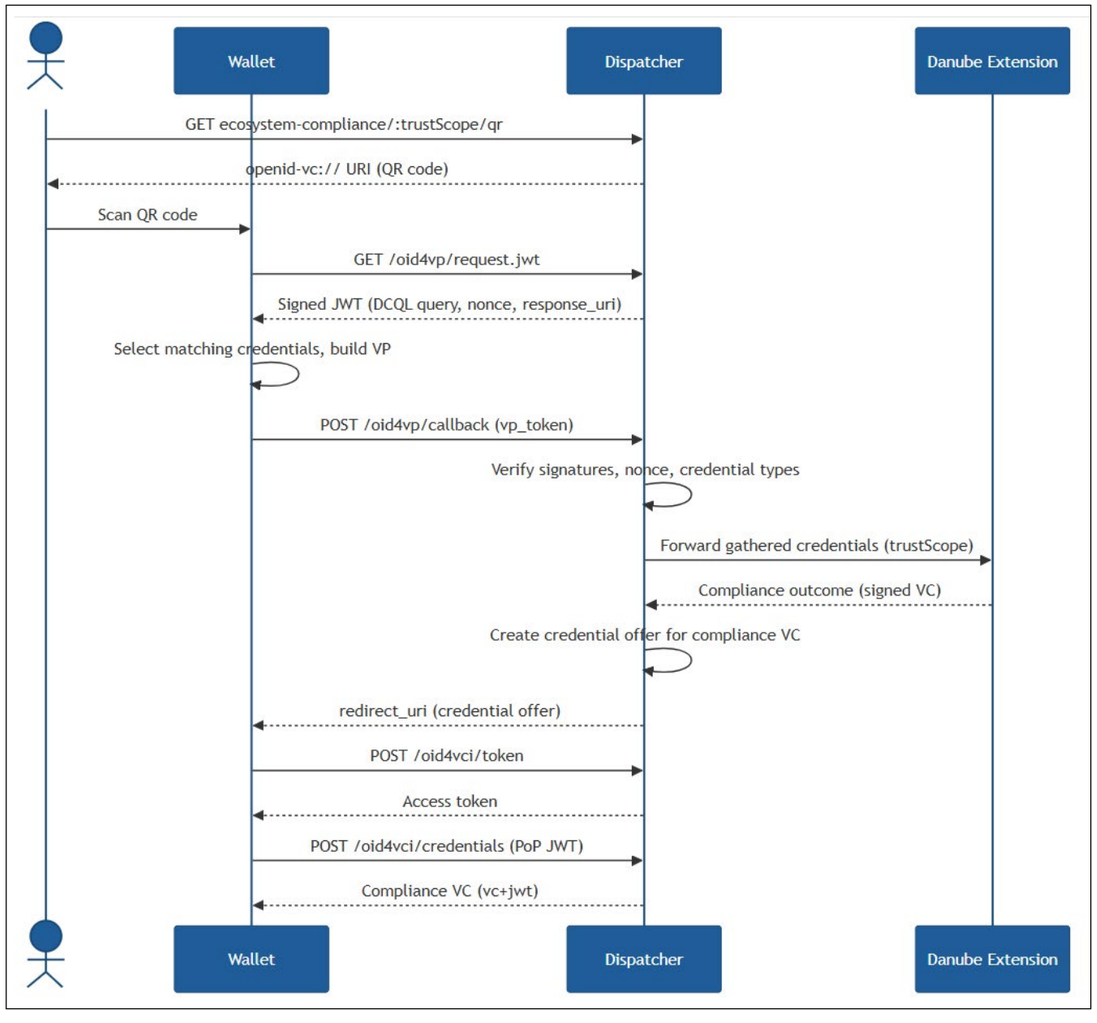
One Scan, Start to Finish

From the user's side, it's a simple and straightforward process. Just one quick scan (or deep link), selecting the requested credentials and waiting for the final credential to be saved in the wallet. No extra work, no extra app to open or form to fill in. Scan and go.

Behind the curtain, the dispatcher chains an OID4VP exchange (gathering the credentials it needs) straight into an OID4VCI issuance (handing back a fresh compliance credential).

It starts with the dispatcher figuring out what it needs from the user to run the compliance check for the selected trust scope. The QR code encodes an openid-vc:// URI, following the JAR pattern (JWT Authorisation Request by Reference): instead of cramming the full request into the QR code, it just contains a request_uri that the wallet fetches separately. That gives a signed JWT with a DCQL query, a nonce, and a response_uri to send the result to.

DCQL (Digital Credentials Query Language) is the bit doing the heavy lifting here. Rather than asking for "a credential" in vague terms, the request includes a DCQL query - a JSON structure where each entry names a credential type and



the expected format. For a Gaia-X Participant Compliance check that means asking for proof of legal identity (gx:LegalPerson), VAT registration (gx:VatID), and acceptance of the Terms and Conditions (gx:Issuer). The wallet evaluates this query against whatever credentials it's holding, picks out the ones that match, and returns them - a structured, machine-readable way of saying "show me exactly these, in exactly this shape," with no back-and-forth needed.

The wallet picks out the matching credentials (with the user's validation), builds a Verifiable Presentation, and posts it as a vp_token to a single /oid4vp/callback endpoint. The dispatcher verifies the presentation, forwards the gathered credentials to the relevant Danube compliance extension, and gets a compliance outcome back - already packaged as a signed VC.

And here's the fun part: instead of just returning that outcome, the dispatcher immediately wraps it in an OID4VCI credential offer and sends it back as a redirect_uri, in the same response. The wallet follows it straight into the credential issuance flow: it exchanges the offer for an access token, then requests the credential with a proof of possession JWT signed by its own key. The dispatcher checks that proof, and hands back the compliance VC exactly as it received it from the compliance extension - untouched and unsigned by the dispatcher itself. Nothing gets tampered with along the way.

Result: a VC JWT lands in the wallet, self-contained and verifiable by anyone who can resolve the issuing extension's DID. No need to contact a centralised authority. One scan in, one portable compliance credential out.

Same Dispatcher, New Tricks

Both legs of the flow lean on the dispatcher's own did:web identity. That one identity covers a few different signing jobs, each with its own short lifespan: the issuer and verifier metadata, the authorisation request JWT the wallet fetches (a 5-minute JAR, typ: oauth-authz-req+jwt), and the verifiable presentation the dispatcher itself builds when talking to the extension. The authorisation request signature is what lets the wallet confirm it genuinely comes from the dispatcher and hasn't been tampered with along the way.

The compliance credential itself, though, comes back already signed by the extension that issued it (Loire, Myrtus, IMX,...). The dispatcher just passes it through as-is rather than re-signing it. Meaning, the dispatcher manages its own keys for everything it puts its name to, but signing compliance outcomes stays firmly with the extension that did the actual evaluation - as it should.

There's also a bit of state to keep track of between the initial QR scan and the vp_token landing later on - handled by Redis with a handful of short-lived, single-use, prefixed keys (nonces, pre-authorised codes, tokens), each consumed atomically so nothing can be replayed.

Trust scope routing itself hasn't changed: the dispatcher reads the trustScope parameter, checks it against the configured TRUST_SCOPES list, and forwards results to the right extension endpoint. Have a look at the latest Architecture Document for more details on the Gaia-X Trust Protocol (which is behind trust scopes) and how it solves the cross-ecosystem trust dilemma. There's also an optional complianceLevel parameter, used by the Gaia-X Loire extension to indicate which label level the check should be run against. The OID4VCI and OID4VP layers just sit on top of that - GXDCH nodes can swap or extend their compliance backends without touching any of the wallet-facing protocol handling. Adding a new compliance extension remains a config change, not a code change.

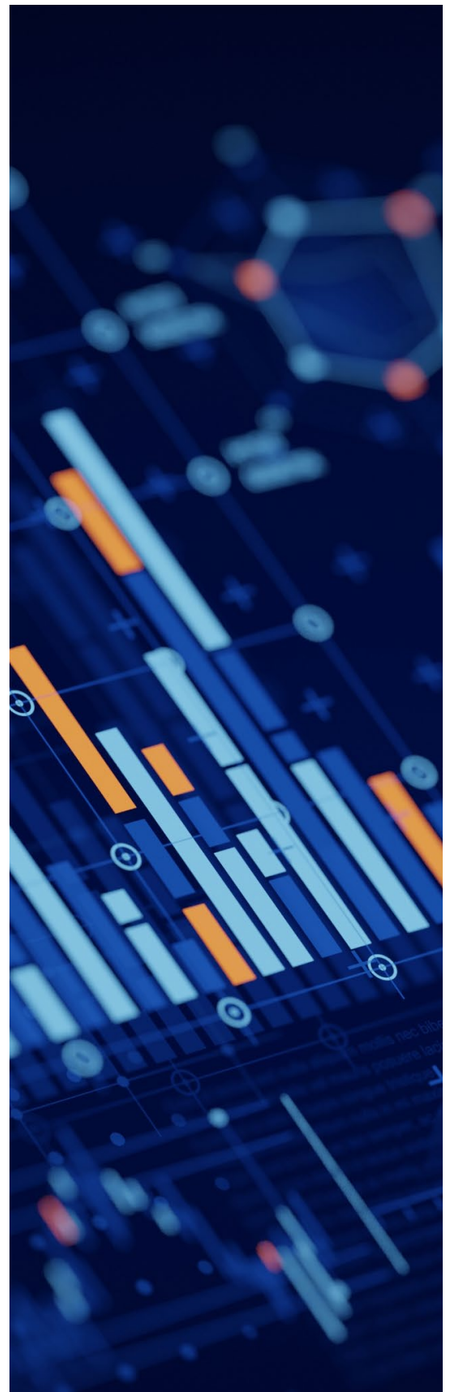
Looking Ahead

Right now, the entry point into the whole flow is a single QR code encoding the openid-vc:// URI - a plain custom-scheme link. That already works well for mobile wallets that register the scheme, but it's also the foundation for where this is headed next: that same URI can double as a deep link, letting web-based wallets expose it directly to their users and skip the QR code altogether. It also opens the door to more automation down the line - think a scripted or headless wallet that walks through the entire flow end to end via that link, making demos and regression testing far quicker than scanning codes by hand.

What This Opens Up

The real win here is **interoperability**. OID4VCI and OID4VP are open standards, so any conformant wallet can take part in the Danube dispatcher's compliance flow. Compliance stops being something that happens quietly in a back-end pipeline and becomes something an organisation can actually carry around, share, and reuse across different contexts and verifiers.

It's a small piece of the puzzle, but it's exactly the kind of portable, user-controlled trust Gaia-X has been aiming for all along.



3.1.4

Bridging Policy, Trust and Verifiable Credentials in Gaia-X Data Spaces

Yassir Sellami, Software Engineer at Gaia-X

From Static Access Rules to Automated Trust-Based Contract Negotiation

As data spaces mature from conceptual frameworks into operational ecosystems, one challenge continues to limit large-scale adoption: how can organisations automatically verify that another participant satisfies access requirements before sharing data, while preserving sovereignty, privacy, and interoperability?

This question sits at the heart of modern data sharing initiatives. In sectors ranging from manufacturing and energy to healthcare and mobility, organisations need to exchange data across institutional boundaries without relying on pre-existing trust relationships. They must be able to prove eligibility, enforce governance rules, and demonstrate compliance in a manner that is transparent, auditable, and machine-processable.

A recent research contribution by Gaia-X Lab Tech Lead Yassir SELLAMI, *Policy-Driven Data Space Contract Negotiation using the ODRL Verifiable Credential Profile and OpenID4VP*, proposes a practical answer. The paper introduces a standards-based protocol that combines policy reasoning, Verifiable Credentials, OpenID for Verifiable Presentations (OpenID4VP), and the Dataspace Protocol (DSP) into a coherent negotiation flow. The result is a mechanism that allows data providers to express access requirements as machine-readable policies and enables consumers to automatically prove compliance using credentials stored in digital wallets.

Beyond its technical contribution, the work is particularly relevant to Gaia-X because it operationalises several core principles of the Gaia-X Trust Framework: trust, interoperability, verifiability, data sovereignty, and compliance-by-design.

Why Data Space Negotiation Remains a Challenge

Data spaces are founded on the idea that data should be shared under conditions defined by the data rights holder. Access is therefore not granted solely based on identity but on whether a participant satisfies specific eligibility criteria.

A provider may wish to share data only with:

- Organisations located within specific jurisdictions.
- Certified participants belonging to a recognized ecosystem.
- Companies holding particular compliance certifications.
- Entities operating under specific contractual obligations.

While such requirements are common, implementing them consistently remains difficult. Policies often describe what must be proven, but they rarely define how proof should be requested, presented, and validated in an interoperable manner.

This creates a gap between policy definition and enforcement.

Organisations frequently rely on manual verification, proprietary integrations, or custom identity systems. Such approaches are difficult to scale and undermine one of the primary objectives of data spaces: enabling automated interactions among previously unknown participants.

The proposed protocol addresses this challenge by establishing a direct connection between policy requirements and verifiable digital evidence.

The Gaia-X Foundation: Trust Through Verifiable Claims

The relevance of this work becomes clearer when viewed through the lens of Gaia-X.

The Gaia-X Trust Framework establishes a common baseline of trust, governance, and interoperability across participating ecosystems. It relies heavily on Verifiable Credentials and machine-readable claims to enable trustworthy digital interactions. Rather than depending on centralised authorities or proprietary trust models, Gaia-X promotes a federated architecture in which trust can be established through cryptographically verifiable assertions.

The Gaia-X Trust Framework explicitly identifies Verifiable Credentials as a cornerstone technology for building trustworthy and interoperable digital ecosystems. These credentials enable organisations to prove attributes, certifications, and compliance claims in a verifiable and decentralised manner.

This aligns perfectly with the protocol proposed in the paper. Instead of asking a participant to submit documents or complete manual onboarding procedures, a provider can simply request cryptographically verifiable evidence corresponding to policy requirements.

The negotiation process therefore becomes an exercise in automated trust evaluation.

ODRL as the Language of Data Governance

A key element of the proposed approach is the use of the W3C Open Digital Rights Language (ODRL).

ODRL has emerged as a foundational policy language for data spaces because it enables organisations to express permissions, prohibitions, obligations, and constraints in a machine-readable format.

The Data Spaces Support Centre (DSSC) and Gaia-X both recognise ODRL as a central technology for expressing usage conditions and governance requirements.

However, standard ODRL alone does not specify how claims about participants should be verified.

This limitation led to the creation of the Gaia-X ODRL Verifiable Credential Profile (ODRL-VC Profile), which extends ODRL by allowing policy constraints to directly reference claims contained within Verifiable Credentials.

For example, a provider can specify that access is allowed only when a credential contains a country code corresponding to France, Belgium, or Spain. The policy no longer refers to abstract concepts but directly to verifiable data contained within credentials.

This transforms ODRL from a policy language into a practical attribute-based access control mechanism suitable for modern data spaces.

Relevant specification:

- Gaia-X ODRL Verifiable Credential Profile: ODRL-VC Profile Specification

Connecting Policy and Proof

One of the most significant innovations presented in the paper is the automatic transformation of policy constraints into credential requests.

The protocol introduces a deterministic mapping between ODRL-VC policies and the Digital Credentials Query Language (DCQL), a standard developed within the OpenID ecosystem.

The process works as follows:

1. A provider publishes an ODRL Offer containing VC-based constraints.
2. A consumer initiates contract negotiation.
3. The provider extracts all policy constraints.
4. These constraints are automatically converted into a DCQL query.
5. The consumer's wallet receives the request.
6. Matching credentials are selected.
7. The wallet presents only the required claims.
8. The provider verifies the credentials and evaluates the policy.
9. If all conditions are satisfied, a binding agreement is issued.

This approach eliminates manual configuration and ensures that the proof request always remains aligned with the governing policy.

Whenever a policy changes, the credential request automatically changes as well.

The result is a powerful reduction in operational complexity and configuration errors.

OpenID4VP: The Missing Operational Layer

OpenID4VP enables a verifier to request credentials from a digital wallet and receive cryptographically protected presentations in response.

The protocol proposed in the paper positions the data provider as an OpenID4VP verifier. During contract negotiation, the provider generates a credential request derived from the policy and sends it to the consumer.

The consumer's wallet then performs credential matching and presents only the information required to satisfy the policy.

This creates a seamless bridge between governance rules and identity technologies.

Privacy by Design and Data Sovereignty

One of the strongest aspects of the proposed protocol is its alignment with privacy and sovereignty principles.

Gaia-X promotes the notion that participants should remain in control of their data and determine when and under which conditions it is shared. The Trust Framework emphasizes transparency, control, and compliance as fundamental ecosystem requirements.

The protocol directly supports these goals through selective disclosure.

Instead of sharing an entire credential, a participant reveals only the claims explicitly required by the policy.

For example, if a policy requires proof that an organisation is located in France, the wallet can disclose only the country code claim rather than the complete organisational profile.

This supports GDPR data minimisation requirements while simultaneously reducing information exposure.

From a sovereignty perspective, the consumer retains control over what to disclose. The wallet presents the requested information only after explicit consent, and the participant remains aware of exactly what information is being shared.

This model represents a significant improvement over traditional onboarding processes that often require excessive disclosure of information.

Integrating with the Dataspace Protocol

Another important contribution of the paper is the integration with the Dataspace Protocol.

DSP already defines how providers and consumers negotiate agreements, exchange offers, and establish contractual relationships. What DSP does not prescribe is how credential-based eligibility verification should occur during negotiation and expecially a common way to express such policies.

The proposed protocol fills that gap.

The authors define a fourteen-step sequence that integrates Verifiable Credential presentation directly into the DSP contract negotiation state machine.

As a result, eligibility verification becomes a native part of contract negotiation rather than a separate external process.

This is particularly relevant for Gaia-X Data Exchange initiatives and future Data Usage Agreement implementations, where contractual obligations and policy compliance must be evaluated before data access is granted.

Governance and Trust Framework Implications

The protocol deliberately separates policy evaluation from trust framework governance.

The ODRL-VC Profile defines what claims are required, but governance authorities must still determine:

- Which issuers are trusted.
- Which credential schemas are accepted.
- How revocation is managed.
- Which trust registries are authoritative.

This separation is particularly important for Gaia-X.

The Gaia-X Trust Framework provides the governance foundation needed to answer these questions. By combining the proposed protocol with Gaia-X trust services and governance rules, ecosystems gain a complete end-to-end model for trustworthy and interoperable access control.

Looking Ahead

The paper arrives at an important moment for the data space ecosystem.

The industry has largely solved the problem of expressing policies. Significant progress has also been made in digital identity standards, Verifiable Credentials, and wallet technologies.

What has been missing is a standardised mechanism that connects these pieces into an operational workflow.

By combining ODRL, Verifiable Credentials, OpenID4VP, DCQL, and DSP, the proposed protocol demonstrates how policy-driven contract negotiation can become fully automated while remaining interoperable and compliant with governance requirements.

For Gaia-X, the implications are significant. The approach offers a concrete path toward automated trust establishment, machine-verifiable compliance, and privacy-preserving access control. It operationalises the principles of sovereignty and interoperability that have guided Gaia-X since its inception and provides a blueprint for future data space implementations in which access decisions are driven not by manual processes but by verifiable evidence and transparent policy evaluation.

As data spaces continue to evolve, solutions that bridge governance, identity, and automation will become increasingly important. This work represents a meaningful step toward that future, bringing the Gaia-X vision of trusted and sovereign digital ecosystems closer to practical reality.

3.2.1

Domain Extensions for Data Spaces: Leveraging the Gaia-X Trust Framework and Trust Protocol for Scalable, Interoperable Data Spaces

White Paper

Roland Fadrany, Chief Operations Officer & **Christoph Strnadl**, Chief Technology Officer at Gaia-X

Executive Summary

The Gaia-X Trust Framework now supports Domain and Geographical Extensions, enabling vertical industries and regional ecosystems to build sovereign, interoperable data spaces under a common trust architecture. Building on it, the Gaia-X Trust Protocol operationalises the establishment of trust between different ecosystems and jurisdictions in a fully interoperable manner.

This white paper outlines the strategic rationale and a concrete implementation proposal for adopting Gaia-X Domain Extensions across vertical and regional data space ecosystems, irrespective of sector or geography.

Key Takeaway

Any established ecosystem is well positioned to act as a domain custodian, retaining full governance over its own credentials and trust anchors while gaining global interoperability with other Gaia-X-technically compliant ecosystems.

Background & Motivation

As data space deployments scale across industries and geographies, a recurring set of challenges has emerged:

- Multiple ecosystems and regions resist reliance on a single, centralised data space operator.
- Regions require their own Participant IDs and Trust Anchors under local sovereign control.
- Cross-data space and cross-ecosystem interoperability is an urgent requirement, particularly along complex value chains and adjacent domains.
- Credentials must be universally verifiable across regions and ecosystems.
- Data spaces need to establish trust with other data spaces and their participants in a rapid and scalable way.
- Onboarding mechanisms must be highly scalable and automated to support rapid growth.

Gaia-X addresses these challenges through a layered extension model that accommodates several coexisting scenarios. Domain Extensions allow individual ecosystems to appoint a custodian — typically an industry or regional governance body — that defines domain-specific rules, certifications, trust anchors, and labels, while maintaining mandatory use of the Gaia-X Participant ID and optional use of Gaia-X Label Levels 1–3.

Building on this, the Gaia-X Trust Protocol provides a universal discovery and automation framework allowing ecosystems to establish unidirectional or mutual trust in a standardised, interoperable way.

The Case for Domain Extensions

Many mature ecosystems are already structurally aligned with the Domain Extension model. Their existing governance bodies effectively function as the domain custodian envisioned by Gaia-X:

- A significant portion of an industry's participants may designate a single body as their custodian and governance authority.
- Such an ecosystem has typically already defined its rules, criteria, certifications, and trust anchors.
- Under Gaia-X 3.0 ("Danube"), a domain custodian does not require Gaia-X Label Levels 1–3, simplifying adoption significantly.
- Domain Extensions can be processed through any Gaia-X Digital Clearing House (GXDCH). Using one or more dedicated, ecosystem-operated GXDCHs that remain fully interoperable with the broader GXDCH network is also possible.

Strategic Benefits of Domain Extensions

Adopting Domain Extensions delivers measurable advantages for ecosystem participants and the broader landscape:

- **Universal recognition**: ecosystem participants become accepted across all cooperating Gaia-X ecosystems.
- **Simplified global expansion**: Geographical Extensions and distributed GXDCHs enable multi-region verification without architectural complexity.
- **Ecosystem growth**: operators can accelerate the onboarding of adjacent industries such as manufacturing, logistics, energy, healthcare, and finance.
- **Clean architectural separation**: a clear boundary between a common Trust Framework and specific functions such as the data space connector, which today solely executes access and usage control policies.

The Case for the Gaia-X Trust Protocol

An ecosystem acting as a data space governance authority may rely on a single, nationally based clearing house for issuing participant and other credentials as the basis for its trust framework.

Such a configuration will meet resistance when interacting with other ecosystems, as they will, in all likelihood, not accept a single foreign clearing house as a trust service provider for their own particular credentials. It may also be the case that non-local clearing houses cannot access and verify foreign identity certificates because of national restrictions — for example, where only national IP addresses or registered national companies are permitted to query company numbers at a national company registry.

The Gaia-X Trust Protocol allows any ecosystem to accredit entities as trust service providers for arbitrary **trust scopes**, not limited to identity or services, nor to any single nationality. Examples include IoT devices, AI agents, data space connectors, machine standards (such as OPC UA), digital product passports, and any identifiable entity. By exposing an ecosystem's list of trust service providers and their respective trust scopes and credentials in so-called **ecosystem trust profiles** within the **Gaia-X Meta-Registry**, it enables one ecosystem (the trustor) to establish selective trust relationships with other ecosystems (the trustee).

Strategic Benefits of the Trust Protocol

Adopting the Gaia-X Trust Protocol enables:

- an ecosystem to keep or extend its current trust profile;
- other ecosystems to establish and keep their own trust profiles;
- an ecosystem to establish unidirectional trust for selected trust scopes with other ecosystems complying with the Gaia-X Trust Protocol;
- other ecosystems to establish unidirectional trust for selected trust scopes in return;
- the establishment of mutual trust between two ecosystems for selected trust scopes; and
- seamless interoperation with other ecosystems at the trust plane.

Proposal & Implementation Path

Gaia-X proposes the following co-creation initiative targeting readiness for the Gaia-X Summit in November:

1. **Co-Create a Domain Extension**. Fully formalise an ecosystem's current credential set within the Gaia-X Domain Extension framework, covering representative credential types such as:
   - » Membership Credential
   - » Participant Identification Credential
   - » Framework Agreement Credential
2. **Deploy a Domain Extension Engine on Danube**. Implement a dedicated extension engine on the Gaia-X 3.0 "Danube" platform, enabling GXDCHs to simultaneously issue and verify both Gaia-X and domain-specific credentials within a single, unified workflow.
3. **Decouple Verification from Access Management**. Separate credential verification (handled by a dedicated clearing house) from access and rights management (handled by the connector). This architectural decoupling improves modularity and cross-ecosystem interoperability, and significantly simplifies the onboarding of new participants through automation.
4. **Demonstrate Cross-Ecosystem Trust using the Gaia-X Trust Protocol**. Use the Danube platform to illustrate how the Gaia-X Meta-Registry and its Ecosystem Trust Profiles enable cross-ecosystem trust — building on proven precedents such as the IMXC use case, the Myrtus data space, available regional company-number extensions, and the generic company-number AI-agent.

Gaia-X Commitment

Gaia-X AISBL is committed to supporting this approach and will provide active technical and governance assistance to ensure readiness in time for the Gaia-X Summit.

Conclusion

The integration of Domain Extensions and the Gaia-X Trust Protocol into any vertical or regional ecosystem represents a natural and strategically sound evolution. By formally adopting the Gaia-X Domain Extension model, ecosystem participants gain global interoperability without surrendering existing governance structures or credential frameworks.

The proposed Domain Extension Engine on Danube provides a technically sound, standards-compliant implementation path that positions any data space for scalable, trusted, cross-industry and cross-region collaboration.

3.2.2

Gaia-X and Quantum Computing

Przemek Halub, Program Manager at Gaia-X

According to an announcement from the European Commission[i], the European Quantum Act proposal is expected in 2026[ii]. It is one of the key initiatives that will establish a strong European position in this field. Now is therefore the perfect time to consider where Gaia-X could fit into the broader area of quantum technologies. Before we move on to the regulatory landscape, let's take a closer look at the practical aspects of quantum technologies and Gaia-X, and consider whether there are any regions where the two could converge.

Quantum technologies relay on subatomic behaviours, where particles exist in multiple states simultaneously (superposition) or remain linked across distances (entanglement). The development of quantum technologies allows us to define new areas where innovative solutions can be applied: quantum sensors, quantum teleportation, quantum communications, and quantum networks for "unhackable" data transfer.

At first glance, quantum computing and Gaia-X may seem unrelated, but upon closer look, it is possible to identify some potential domains that could facilitate connections between the two.

The role of Gaia-X comes to the fore, as a trust framework to guarantee the authenticity and source of data.

Data plays a crucial role in quantum computing, particularly in the context of integration with classical computing systems. Quantum computers require an interface in the form of standard computers through which they can be supplied with data. This area certainly requires further research and clarification as to how such interactions should be organised and structured on many different levels. This seems to be the overarching element where the Gaia-X trust framework can be utilised and implemented. Likewise, we can point to the field of AI, where one of the primary areas of focus this year is the creation of AI participant ID within Gaia-X Trust Framework.

It is also well known, that quantum computing algorithms exist which are able to break several currently widely used data encryption schemes. Even if the exact point in time when this will be available in practice is still somewhat out in the future (best bets in around 7-10 years), all previously stored encrypted data will become decryptable by then. Here, the Gaia-X Trust Framework may be used to identify and attest data sets which are quantum secure, that is, which were encrypted using an algorithm which cannot be broken even by quantum computers.

Given its focus on trust, interoperability and innovative, data-driven solutions, could Gaia-X leverage quantum computing to optimise data processing, analytics and machine learning? While it certainly wouldn't be possible to do so directly, Gaia-X's trust framework could be applied in the background more widely in this area; one of Gaia-X's goals is to enable secure and interoperable data processing, which should foster the development of AI and ML applications. Large learning models are based on data ecosystems and quantum technologies could impact the development of LLMs in the future by overcoming limitations in training efficiency, energy use, and reasoning capabilities. This could lead to significant performance improvements in various sectors, such as image recognition and natural language processing. In future, Gaia-X's federated **data spaces** could also use quantum protocols to enhance privacy and efficiency. So it seems there could be a sweet spot to incorporate quantum communication protocols in the Gaia-X Trust Framework, especially for such fundamental entities like the Gaia-X Registry or the Gaia-X Meta-Registry.

In the context of **infrastructure integration** or **data storage**, quantum computing resources such as processors or simulators could be offered as services within the Gaia-X ecosystem, in a manner similar to current cloud-based classical computing resources. Quantum Computing could be one of the Domain extensions of the Gaia-X framework.

These are preliminary considerations, and specific solutions require a great deal of work and the involvement of experts from various fields and industries.

Compliance and regulations.

In addition to the technical aspects, we should also start considering compliance, policies and rules in the quantum area within the context of the Gaia-X Framework and Gaia-X specifications, especially the Compliance Document. Quantum computing seems to become one of the key technologies in the coming years: the timeframe for this to occur, as stated by the experts, is projected to be beyond 2035.

While Europe does not yet have a binding 'Quantum Act', a clear, published quantum strategy is in place, along with an announced plan to make it legally binding through a future EU Quantum Act[iii].

Several legislative initiatives and existing documents have a significant impact on quantum computing, particularly with regard to security and infrastructure, and shape the regulatory landscape of quantum technology. The EU quantum strategy is a high-level document setting out EU priorities for quantum research, industrialisation, infrastructure, skills and security up to 2030. As previously mentioned, it will form the basis of upcoming legislation, including the Quantum Act, which is on the EU Commission's agenda for 2026 and will see the strategy translated into a binding framework.

In addition to the acts that are not 'only about quantum computing' but establish binding rules that are highly relevant to quantum computing systems, their deployment and transition, some requirements have also been defined in the area of quantum technology and infrastructure[iv]: A detailed review requires additional work and should be carried out as a separate task. In this text, we only indicate those regulations that relate to quantum technologies to a certain extent at this stage:

- EuroHPC Joint Undertaking Regulation (Regulation (EU) 2021/1173) – Legal basis for the EuroHPC JU; EuroHPC procures and operates European supercomputers and now integrates quantum computers as accelerators, often available through cloud like access to European users. LINK: https://eur-lex.europa.eu/eli/reg/2021/1173/oj

- IRIS² secure connectivity programme (Regulation (EU) 2023/588) – Creates the EU secure satellite connectivity system; policy documents describe it as complementary to EuroQCI (European Quantum Communication Infrastructure) and the forthcoming Quantum Act for quantum safe and QKD based communications. LINK: https://eur-lex.europa.eu/eli/reg/2023/588/oj

- Horizon Europe framework (Regulation (EU) 2021/695) – Binding framework for EU R&I funding; within it, the Quantum Technologies Flagship and related calls provide the core EU level legal basis for funding quantum computing, communication and sensing R&D. LINK: https://eur-lex.europa.eu/eli/reg/2021/695/oj

- EU Chips Act (Regulation (EU) 2023/1781) – Semiconductor industrial policy framework that the Commission explicitly links with quantum technologies as part of a broader tech sovereignty package (quantum hardware relies on advanced chip and fabrication ecosystems addressed by this Act). Quantum chips are mentioned in the document. LINK: https://eur-lex.europa.eu/eli/reg/2023/1781/oj

The new months will certainly bring many new discoveries and achievements in the field of cutting-edge technologies. The world will undoubtedly accelerate towards new solutions in the areas of AI and quantum computing . In order to contribute to quantum computing, Gaia-X would need to demonstrate how its Trust Framework supports this area. Of course, there is no doubt that we are still in the early stages of development in quantum field, which means that there are still many question marks. Significant principal technical challenges have to be mastered before they can be fully utilised in production environments. As "quantum pioneers", we are also constantly discovering new applications and possibilities for real-life implementation. However, given the potential here, it seems a good idea to start the discussion and brainstorming on that topic. We won't provide the answers yet, but now is a good time to start asking questions about the role of entire IT ecosystems in the new, upcoming quantum era.

i. Source: https://www.european-quantum-act.com/ 4.01.2026

ii. Source: https://digital-strategy.ec.europa.eu/en/policies/quantum 4.01.2026

iii. Source: https://qt.eu/news/2025/2025-11-04_ec-opens-consultation-on-quantum-act 4.01.2026

iv. Supported by: https://www.perplexity.ai/ 4.01.2026

3.2.3

Europe's Digital Sovereignty: the business opportunity of the AI Economy

Manuel Gutiérrez, Senior Digital Ecosystems Manager at Gaia-X

Beyond Regulation: Europe is building the operating model of the future Digital Economy

For years, digital sovereignty in Europe was largely framed as a defensive necessity linked to reducing technological dependency, protecting sensitive data, strengthening cybersecurity, and responding to the geopolitical implications of relying heavily on non-European digital infrastructures. While those concerns remain relevant, the conversation across Europe is evolving rapidly. Digital sovereignty is no longer emerging merely as a regulatory or governance concept; it is increasingly becoming **the foundation of a new industrial and economic strategy** aimed at shaping how the next generation of digital markets will operate.

This transformation is closely connected to the European Commission's broader vision of Strategic autonomy and European economic and research security, the completion of a true Digital Single Market, and the accelerating ambition behind Europe's AI continent action plan. What is now taking shape is not simply a collection of regulatory initiatives, but the gradual construction of a **trusted digital market architecture** in which interoperability, governance, compliance, digital identity, and sovereign cloud capabilities become structural enablers of economic activity. In this context, digital sovereignty is beginning to function less as a protective shield and more as the operational framework required for Europe to scale AI-driven industrial ecosystems under trusted conditions.

Rather than attempting to isolate itself technologically, Europe is trying to define the governance and trust conditions under which **future digital ecosystems can operate at scale**. This distinction is essential because it shifts sovereignty away from a purely political narrative and reframes it as a market-shaping force capable of creating entirely new economic opportunities.

Why the AI Economy depends on trusted ecosystems

The strategic importance of this shift becomes particularly visible when examining the evolution of the AI economy. Much of the global conversation around artificial intelligence remains focused on models, computing power, and hyperscale infrastructure. Europe, however, increasingly recognises that long-term competitiveness in AI will depend just as much on the ability to operationalise trusted ecosystems capable of connecting data, infrastructure, organisations, and governance frameworks across multiple sectors and jurisdictions.

AI systems derive value from access to large volumes of contextualised and distributed data, yet in highly regulated or industrial environments, that data cannot circulate freely without guarantees regarding governance, usage control, compliance, traceability, and security. As a result, the challenge facing Europe is not simply technological adoption, but the creation of **the trust conditions required for ecosystem-scale collaboration**.

This is precisely where Europe may hold a distinctive advantage. Unlike regions whose digital dominance was largely built around consumer platforms, Europe possesses some of the world's most sophisticated industrial ecosystems in sectors such as manufacturing, mobility, healthcare, aerospace, energy, utilities, logistics, and critical infrastructure. These industries generate enormous amounts of highly valuable operational data, but much of that value remains fragmented inside organisational silos because companies often lack sufficiently trusted frameworks for sharing and operationalising data collaboratively.

The emergence of sovereign digital ecosystems therefore creates an opportunity not only to improve operational efficiency, but also to **unlock entirely new forms of economic value** based on cross-company intelligence, AI-enabled services, federated operational models, and sector-wide digital collaboration.

Sovereignty as a new source of economic value

This is why digital sovereignty is becoming increasingly relevant from a business perspective. Europe is effectively laying the foundations for a new ecosystem economy in which **trust itself becomes an economic enabler**. Sovereign cloud frameworks, interoperable data spaces, digital identity architectures, compliance-by-design mechanisms, and federated governance models are not isolated policy initiatives; together, they form the operational infrastructure required for organisations to participate safely in interconnected digital markets.

In this emerging environment, competitive advantage will not depend exclusively on owning infrastructure or controlling proprietary platforms, but increasingly on the ability to enable trusted participation across complex ecosystems where multiple actors need to collaborate dynamically while preserving operational sovereignty.

The implications of this transition extend across multiple industries and technology domains. Cloud providers, for example, are beginning to compete not only on performance and scalability but also on their ability to provide governance transparency, trusted execution environments, interoperability guarantees, and sovereign operating conditions tailored to highly regulated sectors. Cybersecurity providers are experiencing a similar evolution as security increasingly shifts from perimeter protection toward enabling trusted participation across distributed ecosystems through identity management, policy enforcement, compliance automation, and verifiable trust mechanisms.

At the same time, industrial technology companies are discovering opportunities to monetise operational intelligence through ecosystem-based AI services, industrial data products, predictive coordination platforms, and sector-specific digital marketplaces that generate shared value across value chains. In many respects, **a new services economy is emerging around trust enablement itself**.

The strategic window for European companies

The timing of this transformation is particularly important because Europe is moving rapidly from conceptual frameworks toward operational implementation. Regulations such as the AI Act, the Data Act, NIS2, eIDAS 2.0, and the Cyber Resilience Act are progressively defining the governance conditions under which future digital ecosystems will operate. Simultaneously, industrial AI adoption is accelerating across sectors, sovereign cloud initiatives are gaining momentum, and sectoral data spaces are beginning to move from pilot initiatives toward scalable operational environments.

As these developments converge, **organisations that position themselves early within sovereign ecosystem architectures may gain privileged access to future AI value chains**, trusted industrial marketplaces, and cross-border collaboration environments that are likely to become increasingly strategic over the coming decade.

This context is especially relevant for European companies operating in highly regulated or industrial sectors where trust, compliance, and interoperability are becoming fundamental market requirements rather than optional capabilities. In these environments, participation in trusted ecosystems may ultimately determine which organisations become **orchestrators of future digital value chains** and which remain isolated operators with limited ecosystem relevance.

For smaller European innovators and SMEs, this transition could also represent an important structural opportunity. Federated and interoperable ecosystem models have the potential to reduce dependence on closed, proprietary platforms, allowing specialised players to participate in larger digital ecosystems through shared trust and interoperability standards rather than purely on infrastructure scale.

The role of Gaia-X in Europe's emerging Ecosystem Economy

Within this broader transformation, Gaia-X is becoming strategically important because it helps define the rules of participation for trusted digital ecosystems.

Gaia-X functions primarily as a trust and interoperability framework that enables federated digital environments in which organisations can collaborate securely while maintaining sovereignty and control over their data, services, and operational policies. Its role is therefore not centred on infrastructure ownership, but on **defining the common governance principles, interoperability standards, trust mechanisms, and policy frameworks required for large-scale ecosystem participation**.

This becomes particularly significant in the AI era because industrial AI ecosystems inherently require coordination between multiple actors, including cloud providers, industrial companies, AI developers, infrastructure operators, regulators, and public institutions. Without shared trust frameworks, these ecosystems remain fragmented and difficult to scale across sectors and borders.

Gaia-X addresses this challenge by helping create **the operational conditions necessary for trusted digital collaboration not only at a European scale but also globally**, positioning itself as a coordination layer for the emerging ecosystem economy rather than merely as a technology initiative. For business leaders, this distinction is critical because it changes how Gaia-X should be interpreted strategically. Participation in Gaia-X is not simply about alignment with European policy objectives or regulatory trends; it increasingly represents **an opportunity to position organisations inside the emerging infrastructure of trusted European digital markets**.

Europe's opportunity: leading the global Trust Economy

Europe is therefore pursuing something more ambitious than technological protectionism. It attempts to define the governance and operational architecture of a future digital economy in which trust is embedded directly in the infrastructure of digital collaboration.

While Europe may not dominate every layer of the global AI race, it is uniquely positioned to lead the development of **trusted industrial ecosystems that operate across highly regulated and strategically sensitive environments**.

As AI adoption accelerates across sectors, organisations will increasingly require guarantees around governance, transparency, compliance, interoperability, sovereignty, and operational resilience. In that context, Europe's regulatory philosophy, industrial structure, and ecosystem-oriented approach may evolve into a significant competitive advantage rather than a perceived limitation.

The convergence between Strategic Autonomy, the Digital Single Market, sovereign cloud frameworks, AI industrialisation, sectoral data spaces, and initiatives such as Gaia-X is therefore much more than a policy agenda. It represents the gradual emergence of **a new market architecture for trusted digital collaboration**.

The organisations that recognise this transition early will not simply adapt to the next phase of the digital economy. They may help shape the ecosystems, standards, and trusted infrastructures upon which the next generation of European AI-enabled markets will be built.

3.2.4

Trust as Infrastructure

Gaia-X, Cybersecurity and the Future of Trusted Digital Ecosystems

Manuel Gutiérrez, Senior Digital Ecosystems Manager at Gaia-X

The Shift from Security to Trust

The digital economy is entering a new phase: one defined less by isolated platforms and more by **interconnected ecosystems**. Organisations today rarely operate within clearly bounded technological environments. Industrial companies exchange operational data with suppliers and partners in real time. Public administrations depend on external cloud infrastructures and digital service providers. AI systems increasingly rely on distributed datasets, third-party models and federated computing environments. Critical sectors such as energy, mobility, healthcare and manufacturing are becoming structurally interconnected through data-driven collaboration.

This transformation creates enormous opportunities. But it also introduces a new challenge: **how to scale digital collaboration across ecosystems without losing trust, governance or control**. For years, cybersecurity has been the primary mechanism for protecting digital environments. Its role has been clear: defend systems, reduce vulnerabilities, prevent fraud and ensure resilience against increasingly sophisticated threats. These capabilities remain essential, and no digital ecosystem can function without robust cybersecurity foundations. But ecosystems introduce a different dimension.

Organisations do not collaborate simply because infrastructures are secure. **They collaborate because they trust the conditions under which collaboration takes place**. Cybersecurity protects against malicious behaviour, while trust enables cooperation between independent actors. Security reduces risk, but trust reduces friction. In highly interconnected ecosystems, that friction increasingly becomes one of the main barriers to innovation and scale.

Many organisations already experience this operational reality. Sharing industrial data with external partners often requires lengthy onboarding processes, repeated compliance validations and complex governance negotiations. Cross-border collaboration introduces fragmented trust models, inconsistent identity mechanisms and different regulatory obligations. As organisations become increasingly dependent on external cloud providers, AI services, software components, and interconnected suppliers, trust becomes inseparable from supply chain visibility and governance.

These are no longer theoretical concerns. They are **operational bottlenecks that directly affect how quickly ecosystems can innovate and scale**. This challenge becomes even more visible in sectors where digital and physical infrastructures increasingly converge. In industrial and operational technology environments, organisations must coordinate cybersecurity, governance and operational trust across infrastructures where failures may have physical consequences. Energy ecosystems, manufacturing environments and critical infrastructure operators already face the complexity of coordinating multiple actors, technologies and governance models in real time.

In this context, the challenge is no longer simply securing systems. It is **creating the conditions for trusted participation across ecosystems that remain operationally distributed and organisationally independent**. This fundamentally changes the role of trust.

Traditionally, trust has often been understood as a social, institutional or contractual concept. But in digital ecosystems, trust increasingly becomes operational infrastructure. It becomes embedded into identity mechanisms, governance frameworks, interoperability models, compliance automation and data-sharing policies.

Organisations today already dedicate significant operational effort to validating partners, reconciling compliance requirements, verifying permissions and establishing governance assurances across digital ecosystems. As ecosystems scale, this trust overhead becomes increasingly difficult to manage manually. In other words, **trust becomes something that must be designed, verified and continuously managed**.

Trust as Europe's strategic opportunity

Europe's structural strengths have never been based solely on platform scale. Europe's industrial fabric is deeply ecosystem-oriented, shaped by interconnected supply chains, regulated sectors, public-private collaboration and complex cross-border coordination environments. These characteristics create both complexity and opportunity.

As digital ecosystems become more interconnected, the ability to establish trusted conditions for collaboration may become one of Europe's most important strategic assets. This is where the concept of digital sovereignty begins to evolve beyond infrastructure debates or regulatory narratives. Increasingly, **sovereignty is about the ability to participate confidently in digital ecosystems while maintaining governance capacity, operational visibility and strategic autonomy**.

Organisations today want more than connectivity. They want confidence in how digital ecosystems operate. They want visibility into where data is processed, how AI systems are governed, which policies apply across infrastructures and how dependencies are managed over time. Public administrations and critical sectors increasingly require assurances around interoperability, jurisdictional transparency and operational resilience before engaging in large-scale digital collaboration.

This is not about limiting openness. On the contrary, trusted ecosystems are often the ones most capable of enabling collaboration at

scale because participants have confidence in the underlying rules, governance conditions and operational safeguards. Strategic autonomy, in this context, becomes an enabler of participation rather than a barrier to it.

This is one of the reasons why conversations around sovereign cloud, cybersecurity, trusted infrastructures, operational resilience and AI governance are increasingly converging. They all point toward the same **structural challenge: how to create digital ecosystems that remain open and interoperable while preserving trust, governance and control**.

This broader transition is increasingly visible across the European digital landscape. Initiatives such as the NIS2 Directive, the Cyber Resilience Act, eIDAS 2.0 and the emerging European Digital Identity Wallet are all addressing different dimensions of the same structural challenge: how to establish trusted conditions for participation in interconnected digital ecosystems.

NIS2 strengthens organisational resilience and supply-chain security. The Cyber Resilience Act pushes cybersecurity requirements deeper into the lifecycle of connected products and digital services. eIDAS and the European Digital Identity Wallet establish the foundations for trusted digital identity for citizens and organisations.

Taken together, these initiatives suggest something larger than regulatory evolution alone. They point toward **the emergence of foundational trust layers capable of supporting interoperable, resilient and scalable digital ecosystems across Europe**. Cybersecurity itself is evolving as part of this transition. Increasingly, it is no longer viewed only as a technical discipline focused on protection, but as a foundational layer of ecosystem governance and resilience.

As AI adoption accelerates and critical sectors become more interconnected, this challenge becomes increasingly strategic. The future of competitiveness may depend not only on access to infrastructure or computational scale, but also on the ability to create trusted environments for collaboration and innovation.

Operationalising Trust in digital ecosystems

This is precisely where initiatives such as Gaia-X become strategically significant. Gaia-X can be understood as an attempt to operationalise trust for the next generation of digital ecosystems. Its relevance lies in creating mechanisms that enable organisations to collaborate under transparent, verifiable and interoperable conditions across federated environments.

This includes capabilities related to trusted identity, policy-based data exchange, compliance transparency, interoperable governance and verifiable participation. While these concepts may sound abstract at first glance, they address very concrete ecosystem challenges already faced by organisations today.

Consider an industrial company participating in a multi-partner AI initiative. Data may originate from multiple suppliers, infrastructure providers and operational environments. Governance requirements may vary depending on geography, sector or contractual obligations. Partners may require assurances regarding how data is accessed, processed or reused by downstream participants. Identity validation, policy enforcement and compliance verification quickly become operational challenges rather than purely technical ones. In such environments, trust cannot rely solely on bilateral agreements or manual governance processes because the operational complexity becomes too high.

The same dynamic is increasingly evident across supply chains, where organisations depend on external infrastructure, software providers and interconnected digital services that operate beyond traditional organisational boundaries. As ecosystems scale, organisations need mechanisms capable of dynamically validating not only systems but also identities, claims, permissions, and governance conditions across distributed environments. This is one of the most important transitions currently happening in digital infrastructure: **trust is becoming programmable**.

The evolution of cybersecurity already points in this direction. For years, security models focused primarily on protecting organisational perimeters. More recently, approaches such as Zero Trust architectures shifted the focus toward continuously validating identities, policies and interactions rather than assuming implicit trust within internal networks.

But ecosystem environments require extending this logic even further. The challenge is no longer only securing organisations. It is enabling trusted interactions between organisations that remain operationally independent while still participating in shared digital ecosystems. This requires mechanisms capable of validating identities, enforcing usage policies, verifying compliance claims and ensuring interoperability across infrastructures without generating excessive operational friction. Trust, therefore, evolves from being a static assumption into a dynamic operational capability.

The AI Economy will depend on trusted ecosystems

AI dramatically increases both the value of collaboration and the complexity of trust. Modern AI ecosystems depend on access to distributed datasets, external services, federated infrastructures and increasingly autonomous interactions between systems. As organisations accelerate AI adoption, questions around provenance, explainability, governance and accountability become central operational concerns.

Organisations need confidence not only in the AI models themselves, but also in the ecosystems from which data, services and intelligence emerge. **Trustworthy AI ultimately depends on trustworthy digital ecosystems**.

This is one reason why Europe's broader conversations around AI, cybersecurity, cloud sovereignty and trusted infrastructures are increasingly converging. The emerging strategic vision around Europe's AI future is not limited to computational capacity or model development alone. It also concerns Europe's ability to create trusted environments in which organisations can collaborate, innovate, and deploy AI capabilities

with confidence. **This may become one of Europe's most important competitive differentiators**.

The next phase of the digital economy may not be defined solely by who owns the largest platforms or the largest infrastructure. It may also be **defined by who can create the most trusted ecosystems for collaboration at scale**. That is a fundamentally different way of understanding competitiveness. In the ecosystem economy, organisations capable of participating in trusted environments may benefit from faster onboarding, lower governance overhead, improved interoperability and greater willingness among partners to share data and collaborate on innovation initiatives. Trust reduces friction, and reducing friction becomes economically valuable.

From this perspective, cybersecurity also evolves strategically. Its role is no longer limited to defending systems from external threats. Increasingly, **cybersecurity becomes part of a broader architecture of confidence that enables organisations to interact safely across distributed ecosystems**. In interconnected environments, resilience increasingly depends not only on protecting individual organisations, but also on establishing **trusted coordination mechanisms across entire value chains and digital ecosystems**.

This distinction matters because the future of digital ecosystems will not depend only on technological performance. **It will depend on participation**. Ecosystems generate value when organisations are willing to collaborate, exchange data, integrate services and co-create innovation across organisational boundaries. And participation ultimately depends on trust.

Perhaps this is the deeper significance of initiatives such as Gaia-X. They are not simply interoperability initiatives or governance frameworks. They are early attempts to build **the trust infrastructure required for the next generation of digital ecosystems**. Because ultimately, the ecosystems capable of generating trusted interactions at scale may become the ecosystems that attract innovation, collaboration and long-term economic value. Cybersecurity protects the digital economy from failing, but trust is what enables it to scale.

3.3.1

The Data Spaces Support Centre enters phase two to scale European data spaces

Communications Team, Gaia-X

Last month, the Data Spaces Support Centre (DSSC) officially launched its second phase during a kick-off meeting at the Fraunhofer office in Brussels, marking an important new chapter for the European data spaces ecosystem.

Running over the next three years, this phase brings together a renewed consortium of leading European organisations united by a shared ambition to accelerate the development and adoption of data spaces across Europe. Building on the achievements of the first phase, the DSSC is now moving into a stage focused on scaling impact and delivering real value.

The first phase laid essential groundwork through the development of technology stacks, the creation of vibrant ecosystems, and the delivery of feasibility studies and pilot projects. Now, the focus shifts towards stability and expansion, with a clear emphasis on growth, business viability, and return on investment. By strengthening value propositions and incentives for participants, the DSSC aims to unlock broader adoption and long-term sustainability.

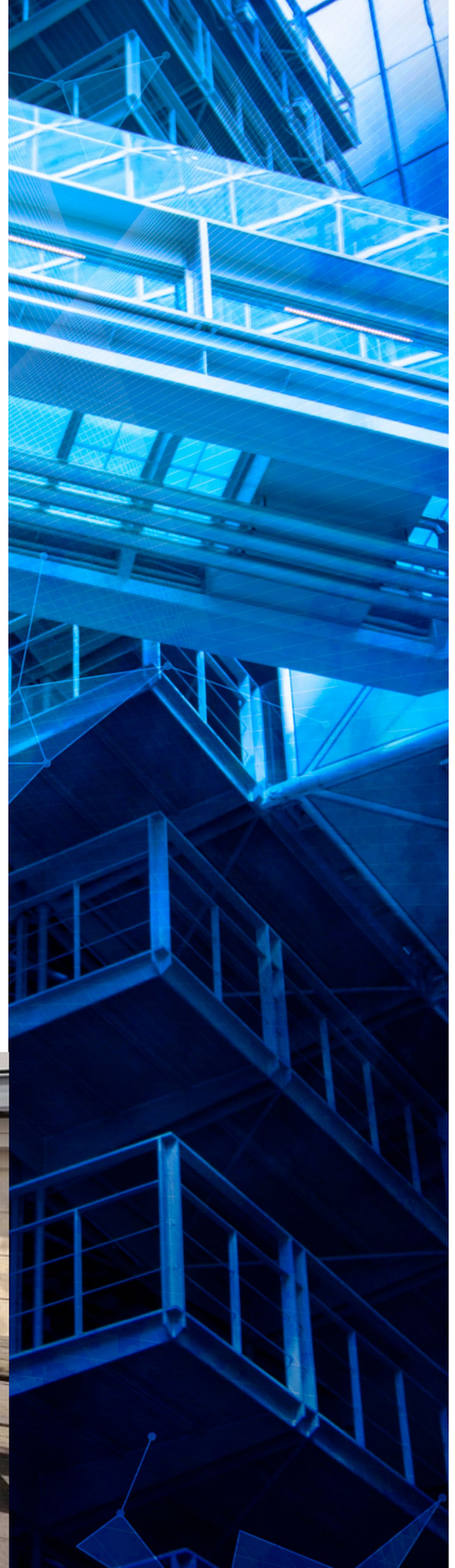
A key priority will be to accelerate network effects while addressing remaining technical and infrastructural challenges. These efforts will support stakeholders in operationalising data spaces at scale and unlocking new opportunities for cross-sector collaboration.

At the heart of this phase lies a strong commitment to building a sustainable European data economy. By enhancing productivity, promoting existing assets, and supporting the continued growth of data-driven innovation, the DSSC is set to play a central role in shaping Europe's digital future.

The DSSC will also deepen engagement with data-sharing communities and strengthen collaboration across the AI, cloud, standards, and research ecosystems. This work is closely aligned with broader European initiatives, including the European AI Continent Action Plan, with a particular focus on enabling the integration of AI Factories and their data labs with Common European Data Spaces.

The launch of this second phase is more than a milestone. It is a signal of momentum, ambition, and collective commitment to making data spaces a reality at scale across Europe.

For more information, visit: https://dssc.eu/



04

COMMUNITY

The Gaia-X Community plays an instrumental role in shaping our organisation. This section celebrates and highlights the invaluable contributions made by Gaia-X Hubs, Lighthouses and Members and showcases their stories, expertise, and the remarkable impact they have had on our journey. We will explore their innovative solutions, industry insights, and the collaborative projects that have propelled us forward. As we embark on this exciting journey of showcasing our community, we extend our heartfelt appreciation to every one of them. Their dedication, expertise, and unwavering belief in our shared goals have been instrumental in propelling us towards greater heights.

Members Stories
Hub Highlights
Lighthouse Updates

04

4.1.1 Dawex

From Standard to Open Source Stack: Implementing Trusted Data Transactions with the Gaia-X Framework and the Data Transfer Agent

Benoit Tabutiaux, Chief Technology Officer at TeraLab - IMT Transfert & **Frederic Bellaiche**, Vice President of Technology and Research at Dawex

At Gaia-X Tech-X 2026 in Athens, experts took the stage to tackle one pressing question in European data exchange: how do you make a data exchange genuinely trustworthy, not just technically, but legally and operationally? Benoît Tabutiaux, CTO at IMT Transfert – TeraLab, Frédéric Bellaiche, VP Technology & Research at Dawex, joined Christoph Strnadl, CTO at Gaia-X, and walked attendees through a concrete blueprint mapping the new TDT harmonised European standard to the Gaia-X Framework and the open-source Data Transfer Agent. Here is an overview of their presentation.

As data spaces scale from pilot projects to real-world industrial deployments, one question has moved from theoretical to urgent: what does it actually take to make a data exchange trustworthy, not just technically, but legally and operationally? The new harmonised European standard Trusted Data Transactions answers this question with rigorous precision. And an open-source software component called the Data Transfer Agent (DTA) turns that answer into running code.

The Standard: Trusted Data Transactions (TDT)

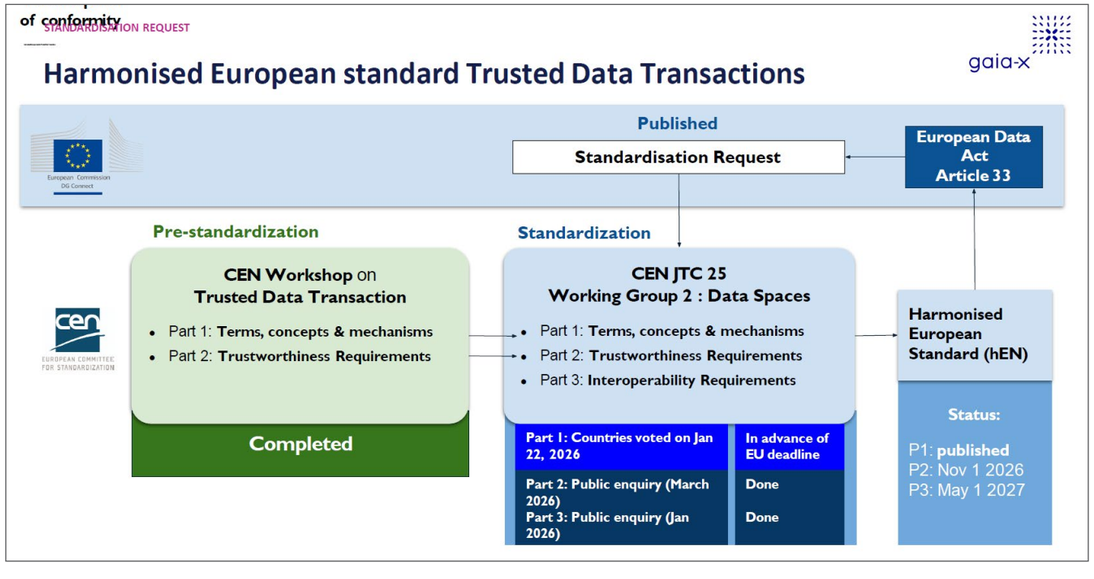
The Trusted Data Transactions (TDT) standard, formally EN 18235, is a harmonised European standard developed at the European Commission and CEN/CENELEC level, directly mandated by Article 33 of the European Data Act. TDT defines the trust criteria that any cross-ecosystem data transaction must comply with to be considered genuinely trustworthy.

The standard identifies **six phases** that every trusted data transaction must satisfy:

1. **Grant Rights**: Traceable delegation records, metadata on allowed users and purposes, provenance and consent for personal data.
2. **Publication**: Verified publication rights, machine-readable catalogue metadata, licence terms, and data quality descriptors.
3. **Discovery**: Access-controlled exposure of data products, with results enabling assessment of relevance and licence terms.
4. **Negotiation**: Provider-evidenced authority to license; contracts recorded in machine-readable, undisputable form.
5. **Data Sharing/Exchange**: Identity verification of the data user, authorisation evaluation, compliance with observability mechanisms.
6. **Access & Usage**: Re-verification of authorisations on each access, ability to revoke supply on breach, observability throughout.

Identity verification, policy and claims reconciliation, and observability apply continuously across every phase, not just at the point of transfer.

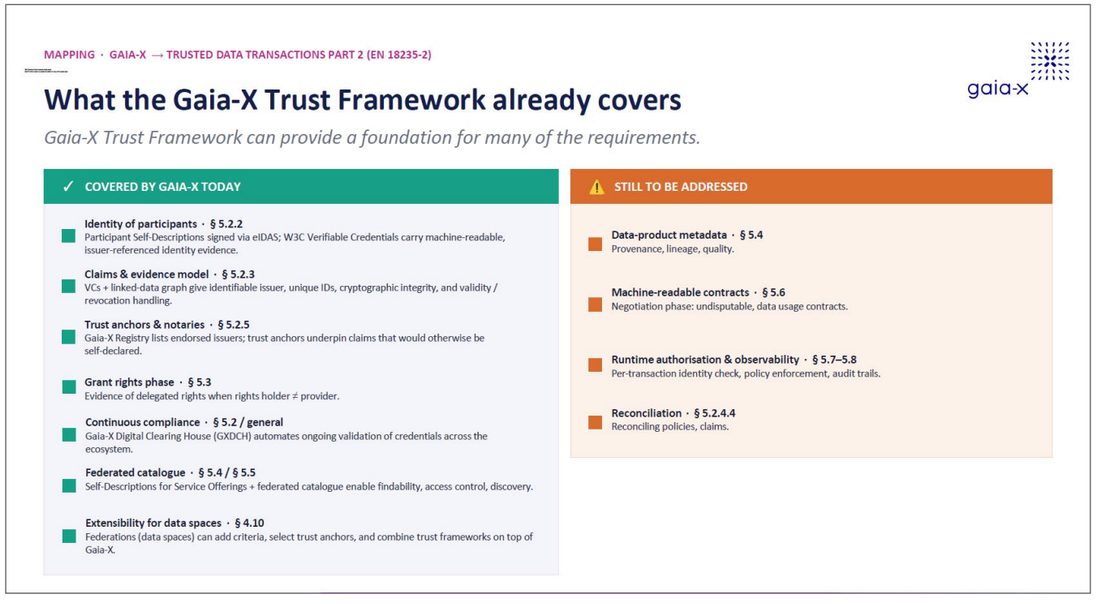
- Part 1 of the standard (EN 18235-1:2026) on Terminology, Concepts and Mechanisms, was made available in March 2026, as part of the harmonised European standard.
- Part 2, addressing Trustworthiness Requirements, entered public enquiry in March 2026.
- Part 3, covering Interoperability Requirements, entered public enquiry in May 2026.



Gaia-X Framework: A Solid Foundation for TDT

The Gaia-X Trust Framework already satisfies a significant share of TDT requirements. From identity to continuous compliance, key building blocks are already in place.

- **Participant identity (§ 5.2.2)**: Participant Self-Descriptions signed via eIDAS, combined with W3C Verifiable Credentials, deliver machine-readable, issuer-referenced identity evidence that satisfies TDT's identification requirements out of the box.
- **Claims and evidence model (§ 5.2.3)**: The Verifiable Credentials plus linked-data graph model provides identifiable issuers, unique identifiers, cryptographic integrity, and built-in validity and revocation handling, precisely what TDT demands from any policy, claim, or evidence artefact.
- **Trust anchors and notaries (§ 5.2.5)**: The Gaia-X Registry lists endorsed issuers and trust anchors, underpinning claims that would otherwise be purely self-declared.
- **Continuous compliance (§ 5.2 / general)**: The Gaia-X Digital Clearing House (GXDCH) automates ongoing validation of credentials across the ecosystem, enabling the continuous compliance posture TDT requires.
- **Federated catalogue (§ 5.4 / § 5.5)**: Self-Descriptions for Service Offerings, combined with a federated catalogue, enable findability, access control, and discovery aligned with TDT's publication and discovery requirements.
- **Extensibility for data spaces (§ 4.10)**: Federations (i.e. data spaces) can layer additional criteria, select their own trust anchors, and compose trust frameworks on top of Gaia-X, precisely the kind of modular trust framework architecture TDT envisions.



Bridging the Last Mile to TDT Compliance

While Gaia-X covers the trust infrastructure, a focused set of requirements calls for dedicated work and attention:

- **Data-product metadata (§ 5.4)**: Provenance, lineage, and quality descriptors at the data-product level require new ontologies to be introduced into the Data Product Model.
- **Machine-readable contracts (§ 5.6)**: Undisputable, machine-readable data usage contracts for the negotiation phase require dedicated specification work, currently underway in Gaia-X's Data Exchange Services working group.
- **Runtime authorisation and observability (§ 5.7–5.8)**: Per-transaction identity checks, real-time policy enforcement, and audit trails, the operational heart of TDT, are not yet fully specified in Gaia-X.
- **Reconciliation (§ 5.2.4.4)**: Reconciling policies and claims across participants and intermediaries requires tooling beyond what the Trust Framework alone provides.
- **Grant rights phase (§ 5.3)**: Evidence of delegated rights when the rights holder is not the data provider.

This is precisely where the Data Transfer Agent comes in.

The Data Transfer Agent: Operationalising TDT

The Data Transfer Agent (DTA) is an open-source software component purpose-built to enable trusted data transactions in data spaces, by offering a lightweight, containerised agent that any organisation, regardless of size, can easily deploy and operate with trust.

DTA comes into play once two parties have agreed on a data transaction. Its role is to carry out all the verifications and operational steps needed to execute that transaction in a TDT-compliant way.

Concretely, the DTA handles:

- **Participant, data product, and Data Access Contract (DAC) management**
- **Policy enforcement and access granting**
- **Data transfer and streaming**
- **Observability**, logging and audit trails for non-repudiation

The component implements the Gaia-X Trust Framework and the **OIDC4VC/OIDC4VP** OpenID standards, ensuring that every interaction is grounded in verifiable credentials and interoperable identity protocols.

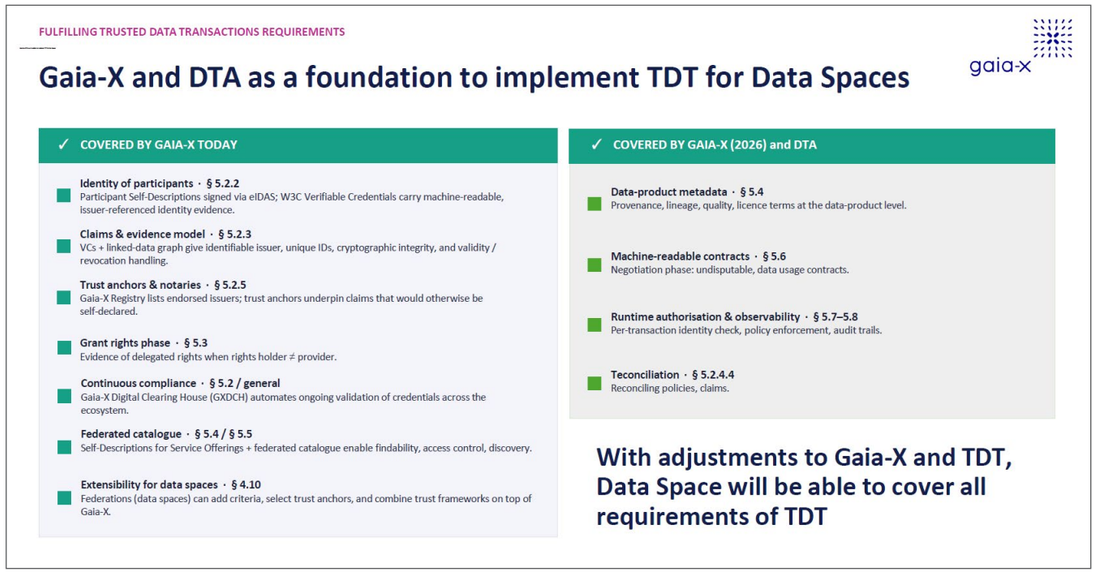
Key characteristics of the Data Transfer Agent include:

- **Lightweight and modular**: Uncluttered architecture focused exclusively on trusted data transactions, with no unnecessary complexity.
- **Standards-compliant**: Built in full alignment with Gaia-X specifications, the CEN Trusted Data Transactions harmonised European standard, and the European Data Act.
- **Distributed by design**: Deployable across cloud, on-premise, edge environments; can run as a managed service alongside any existing component or software
- **Open source**: Released under Apache-2 license on the Gaia-X GitLab, with transparent governance and no dependency on any single vendor or data space
- **Scalable**: Capable of supporting thousands of participants across complex industrial supply chains, from large enterprises to SMEs
- **Human-in-the-loop ready**: Supporting both fully automated machine-to-machine transactions and workflows requiring human consent or validation, a critical capability required in highly regulated sectors
- **Built for Agentic AI**: Designed to support the evolving pace of automated data interactions, with an extensible architecture that accommodates new communication modes and use cases as they emerge

The Complete Picture: How Gaia-X and the DTA Cover Every TDT Requirement

Combining the Gaia-X Trust Framework with the DTA closes the remaining gaps:

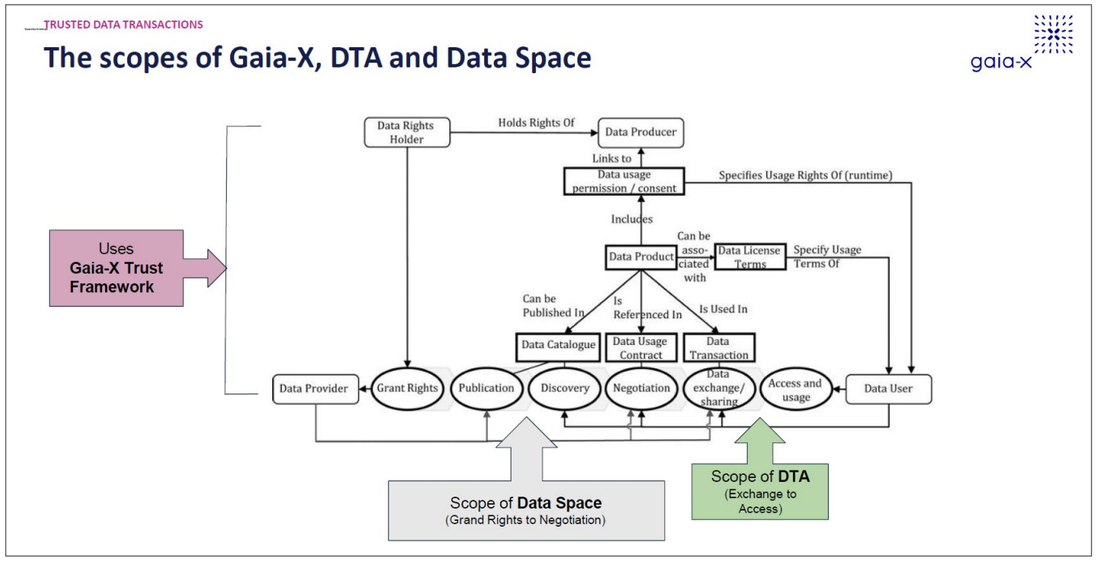
TDT Requirement	Covered by
Participant identity (§ 5.2.2)	Gaia-X (eIDAS + Verifiable Credentials)
Claims & evidence model (§ 5.2.3)	Gaia-X (VC + linked-data graph)
Trust anchors & notaries (§ 5.2.5)	Gaia-X Registry
Continuous compliance	Gaia-X Digital Clearing House
Federated catalogue (§ 5.4–5.5)	Gaia-X Self-Descriptions
Runtime authorisation & observability (§ 5.7–5.8)	DTA
Reconciliation (§ 5.2.4.4)	DTA
Machine-readable contracts (§ 5.6)	DTA (pending Gaia-X specification)
Data-product metadata / provenance (§ 5.4)	Ongoing Gaia-X work (new ontologies)
Grant rights evidence (§ 5.3)	Ongoing Gaia-X work



Aimed at addressing the realities of industrial data spaces, removing integration complexity and associated deployment costs, DTA is designed from the ground up with a modular, scalable architecture. Ultimately, this translates into concrete operational benefits: easy deployment across on-premise, SaaS, or edge environments; straightforward monitoring and auditability; seamless updates; and the ability to participate in multiple data spaces simultaneously without vendor lock-in.

What Comes Next

The foundation is in place, and the momentum is real. Gaia-X working groups are actively completing the remaining pieces: new ontologies for data products, the Data Access Contract specification, and an observability framework. Each step brings the full vision of TDT-compliant data spaces closer to reality. This is an open, collective effort.



Join the DTA Open Source Community

The DTA source code is available on the Gaia-X GitLab under an Apache 2.0 licence. Organisations across industries are invited to contribute.

Useful links

- Gaia-X Tech-X presentation: https://gaia-x.eu/wp-content/uploads/2026/06/TX26_TrustedDataTransactions_GaiaX-FInal-29-05-2026.pdf
- Gaia-X Tech-X recording: https://www.youtube.com
- Gaia-X Trust Framework: https://docs.gaia-x.eu/technical-committee/architecture-document/25.11/trust_framework_architecture/
- Trusted Data Transactions harmonised European Standard – Part 1: https://www.cencenelec.eu/news-events/news/2026/en-in-the-spotlight/2026-04-30-en-18235-1-2026-data/
- Data repository: https://gitlab.com/gaia-x/gaia-x-community/data-transfer-agent

4.1.2 ITG

The Industrial Data Space of Galicia: building bridges towards sovereign data sharing

Diego Campelo Cores, Technical Lead & **Antonio Carreiro Alonso**, Technical Manager at ITG

Galicia, a region on the Atlantic coast of northwestern Spain, historically developed an industry closely tied to its local resources and needs in order to adapt to its isolation and distance. From that context emerged a diverse industrial ecosystem, deeply connected to the produce of the land and the sea, which today faces a challenge common to all of European industry: competing in an increasingly digitalised environment, where data sharing has become essential for productivity and innovation across the entire value chain.

Within this framework, ITG, together with DIHGIGAL and under an agreement with IGAPE, is driving the Industrial Data Space of Galicia with a clear aim: to build bridges towards secure, sovereign and efficient data sharing within the Galician business fabric. The initiative connects some of the region's major economic engines: the renowned food sector, the historic shipbuilding industry, the international automotive sector and the growing ICT ecosystem.

Sharing data effectively requires that both companies and their teams understand the advantages and incentives of doing so. For this reason, the Industrial Data Space of Galicia is conceived not merely as a technological infrastructure, but as a context for cooperation capable of generating new opportunities for innovation and research. Through its marketplace, it facilitates the discovery of previously inaccessible resources and opens up new business opportunities, governed by a data sovereignty model that legally guarantees the obligations and restrictions of each exchange, so that every company retains control over its own information.

Alignment with the principles of Gaia-X reflects the need to build an ecosystem based on interoperability, trust and digital sovereignty, following European standards for data spaces. In doing so, the initiative becomes part of a continental movement that seeks to enable small and medium-sized industrial enterprises, too, to join emerging data ecosystems with confidence, lowering the technical and knowledge barriers that often hold back their adoption.

Conclusion

The expected impact is manifold: enabling Galician companies to put underused data to work while retaining control over its use, reducing adoption barriers and unlocking new opportunities for innovation through access to information that was previously out of reach. The next steps focus on onboarding participants across the four sectors, expanding real use cases and consolidating alignment with the Gaia-X Trust Framework. Galician industrial companies are invited to take part and help shape an ecosystem built on cooperation, trust and data sovereignty, strengthening the capacity of Galician industry to adapt and thrive in an increasingly digital landscape.

ITG was delighted to sponsor the Data Spaces Symposium 2026 in Madrid, where the many valuable contacts made are already helping to strengthen Galician industry's capacity to adapt and thrive in an increasingly digital landscape.

Diego Campelo Cores
Technical Lead at ITG

Antonio Carreiro Alonso,
Technical Manager at ITG

4.1.3 EIT Manufacturing East

From principle to practice: The “COMPLIANCE4DPP” project makes compliance operational for Digital Product Passports in Gaia-X data spaces

Carola Wisbar, Authorised Signatory (Prokurist) & **Theresa Neuhauser**, Senior Manager - Communications, both at EIT Manufacturing East GmbH

Digital Product Passports are moving from policy discussion to practical implementation. For European industry, they create both an obligation and an opportunity: companies must manage more product data, meet growing regulatory requirements and exchange information across complex value chains, while also unlocking transparency, circularity and new data-based services.

COMPLIANCE4DPP, a new Horizon Europe-funded project launched on 1 June 2026, aims to turn Gaia-X principles into practice by developing automated compliance tooling for trusted Digital Product Passport implementation and interoperable data exchange across industrial value chains.

The Digital Product Passport is the main showcase, but the approach is broader: compliance should become a reusable capability for data ecosystems, not a one-off administrative exercise. Gaia-X is central to this ambition. COMPLIANCE4DPP builds on Gaia-X principles and the “Bring Your Own Rules” approach, enabling communities to define and apply their own compliance requirements while remaining interoperable.

As **Johannes Hunschofsky**, Managing Director of the project coordinator EIT Manufacturing East GmbH, puts it: *“Everyone talks about data spaces, Digital Product Passports and trusted data sharing. The real challenge is making them work in practice. Gaia-X has created an important foundation by establishing common principles for trust, transparency and interoperability. The next step is helping organisations put these principles into operation across real-world value chains. That is where COMPLIANCE4DPP comes in. We want to make compliance easier to manage, less resource-intensive and more scalable across organisations and ecosystems. The project will not only support the adoption of Digital Product Passports but also help companies collaborate more confidently within European data spaces. Ultimately, we aim to turn trust and compliance into drivers of innovation rather than barriers to it.”*

A central project objective is “Compliance by Design” through open tooling: policy generation, validation and enforcement based on Policies-as-Code, supported by user-friendly interfaces for authoring and testing. The project also contributes Free and Open-Source Software components. Building on Pontus-X, a Gaia-X Lighthouse Data Space, it aims to advance towards production-grade DPP integration.

Helmut Leopold, Chairman of the Gaia-X Hub Austria and Head of Centre for Digital Safety & Security at AIT Austrian Institute of Technology, adds: *“Gaia-X services for automated on-boarding in federated data spaces and Digital Product Passport concepts are pre-requisites for data sovereignty and enhanced cybersecurity as these services enable automated permanent compliance verification of data and IT-services.”*

For SMEs, the project addresses an urgent need. **Martina Le Gall Maláková**, President at INDUSTRY INNOVATION CLUSTER and Chair at SMEs and Entrepreneurs Committee at Business at OECD, states: *“As Chair at SME and Entrepreneurship Committee at Business at OECD, I know how important it is to deliver digital solutions that strengthen the competitiveness of European SMEs. These solutions must be user-friendly, transparent, efficient, and automatically aligned with*

EU legislation in this age of AI and big data. This is the goal of COMPLIANCE4DPP. All partners from the consortium are strongly committed to achieving this goal and delivering meaningful benefits for SMEs."

Although COMPLIANCE4DPP has only just started, its ambition is clear: to help European industry move from regulatory obligation to operational value.

Stay up to date with COMPLIANCE4DPP by following us on LinkedIn: https://www.linkedin.com/company/compliance4dpp

About COMPLIANCE4DPP

Coordinated by **EIT Manufacturing East GmbH**, COMPLIANCE4DPP is implemented by a European consortium of 19 partners from nine countries:

- AIT Austrian Institute of Technology GmbH
- Assist Software SRL
- Associação Para O Polo Das Tecnologias Da Informação, Comunicação E Electrónica TICE.PT
- Atlantic Technological University
- DeltaDAO AG
- EIT Manufacturing East GmbH
- Fundacion Centro De Tecnologias De Interaccion Visual Y Comunicaciones Vicomtech
- Gaia-X European Association for Data and Cloud AISBL
- GOIMEK S. Coop.
- IDEKO S. Coop.
- INI-Novation GmbH
- Lansky, Ganzger, Jacko & Partner, s.r.o.
- Macedonian Enterprise Development Foundation Skopje
- Posedio GmbH
- INDUSTRY INNOVATION CLUSTER
- soffico GmbH
- Talleres Wolco S.L.
- Technische Universität Darmstadt
- Technische Universität Wien

Together, the partners contribute expertise in Gaia-X data spaces, Digital Product Passports, industrial data ecosystems, regulatory compliance, open-source tooling, circular manufacturing, SME engagement, communication and exploitation.

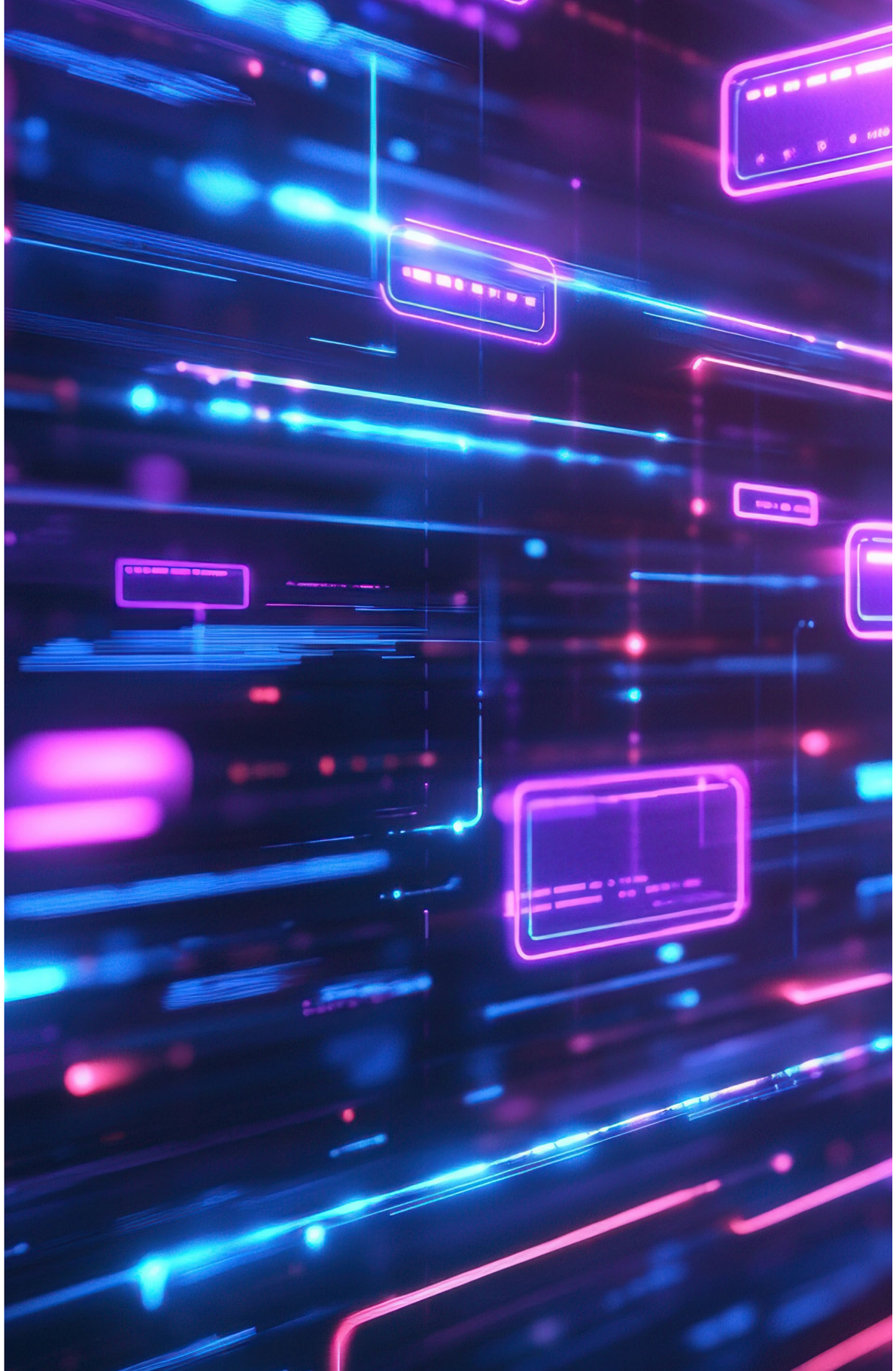
Acknowledgement: This project is funded by the European Union under Horizon Europe Grant Agreement No. 101298718 – COMPLIANCE4DPP.

Media contact:

Dominique Garcia Marschall

EIT Manufacturing East GmbH - Strategic Projects Manager

dominique.garciamarschall@manufacturing.eu



4.2.1 Hub France

Gaia-X Hub France Releases Technical Booklet on Digital Wallets

Christophe Boutrou, Responsable Communication, TeraLab

The **Gaia-X Hub France** is pleased to announce the publication of its technical booklet: **"Digital Wallets at the Core of Trust in Data Spaces."** This comprehensive resource stems from a high-level workshop held on October 7, 2025, which brought together key stakeholders to explore the future of identity and sovereignty, and the current state of the art in wallet technologies within the European data ecosystem.

Why Digital Wallets Matter for Gaia-X

In the architecture of data spaces, identity management and compliance are the fundamental pillars ensuring secure data exchanges and participant sovereignty. The booklet explores the paradigm shift towards **Self-Sovereign Identity** (SSI), a decentralised model that grants users (whether individuals, legal entities, or connected objects) full control over their digital credentials without relying on centralised authorities.

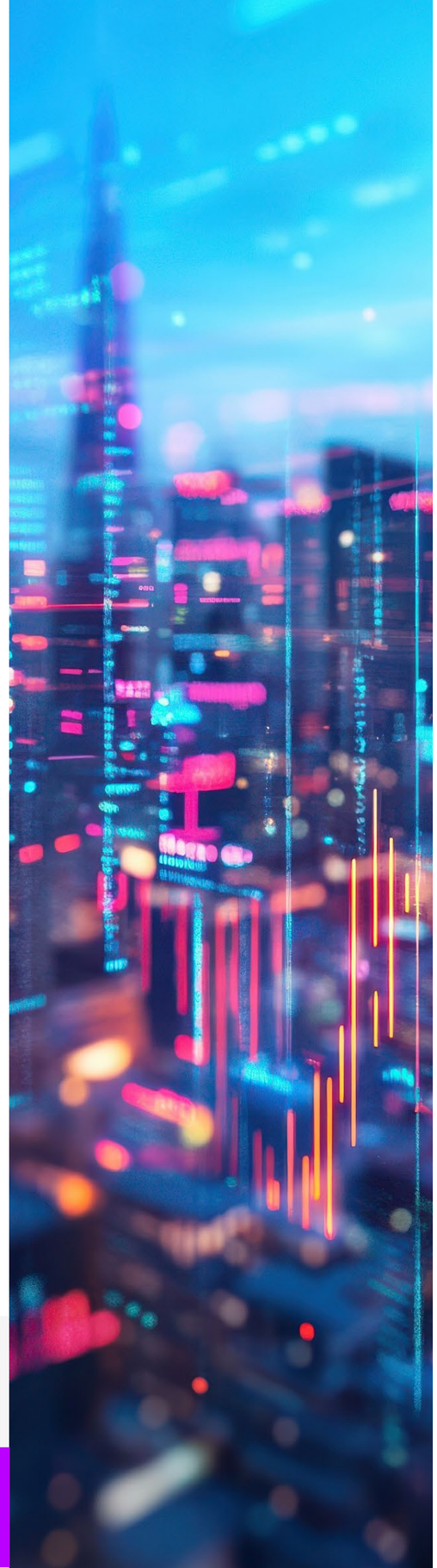
From Theory to Large-Scale Implementation

The publication bridges the gap between theoretical frameworks and industrial reality. It features expert contributions on:

- **The SSI Revolution**: An exploration of the transition from siloed identity models to user-centric ecosystems, illustrated by the **TracIA project** for dynamic patient consent in healthcare.
- **Regulatory Alignment**: A deep dive into the **eIDAS v2** regulation and the upcoming **European Digital Identity (EUDI) Wallet**, which will provide the legally recognised trust services necessary for scaling data spaces across Europe.
- **Industrial Use Cases**: Concrete feedback on "Object Wallets" for vehicle health logs, consent management, and the modernisation of transport and logistics through the **My Hub Pro** solution.

This publication brings together diverse expertise from leading industrial and academic actors **(Télécom SudParis, Atos Eviden, Docaposte, Orange Business, IN Groupe)** who shared their insights and real-world implementations. Gaia-X Hub France is coordinated by Institut Mines-Télécom with the support of Cigref. The "Digital Wallets at the Core of Trust in Data Spaces" booklet is now available for download on the Hub France website: https://www.gaia-x-hub.fr/wp-content/uploads/2026/05/GaiaX_Wallet_E4.pdf

Gaia-X Editorial Note: To go further on the topic, check here to find out more about what the Gaia-X Lab has produced about wallets.



4.2.2 **Hub Netherlands**

Sovereignty at the core: how the Netherlands is contributing to Europe's cloud future

Muriel Sinselmeijer, Project Manager Marketing and Communications at Centre of Excellence for Data Sharing & Cloud

Cloud sovereignty is at the heart of the recent activities of the Dutch Gaia-X Hub, represented by the Centre of Excellence for Data Sharing & Cloud (CoE-DSC). After years of focus on vision and principles, attention is now clearly shifting towards adoption, scalability and interoperability. The past months show that the Netherlands is not only contributing ideas but is also actively helping to build European solutions for a sovereign cloud.

Data Sharing Festival – Sovereignty: from principle to practice

During the Data Sharing Festival in Rotterdam, more than 300 professionals from the Netherlands and abroad came together for two days of sharp insights, open conversations, collaboration and concrete examples around the theme of sovereignty.

The festival highlighted that organisations increasingly require a cloud environment in which control over data, transparency and trustworthy governance are central. Gaia-X is seen as a crucial building block in achieving this. Sectors can only share data safely and responsibly when they jointly invest in shared frameworks such as the Gaia-X Trust Framework, interoperability and privacy-enhancing technologies.

The conclusion was clear and echoed throughout the event: action is needed now and the only way to success is through collaboration. Download the keynote presentations and watch the after movie, including a contribution by Gaia-X CTO Christoph Strnadl: Data Sharing Festival 2026 - Centre of Excellence for Data Sharing & Cloud.

Success for the Dutch team at Gaia-X Tech-X & Hackathon 2026 in Athens

For the third year in a row, a podium finish for CoE-DSC at the Gaia-X hackathon! The team won the first prize with the development of a neuro-symbolic workflow that combines different types of AI to enable a smart search function in digital marketplaces, automatic checks on whether services are compatible (e.g. SaaS and PaaS), and the assessment of provider reliability. This contributes to trustworthy collaboration between services and strengthens European digital sovereignty in an innovative way.

Another successful Dutch contribution in Athens was the presentation of the Myrtus Trust Framework now being part of Gaia-X Danube, the new Gaia-X compliance system. This marks an important step towards standardisation and interoperability between systems: supporting trusted onboarding and verification of new participants in the ecosystem. The solution can be tested via an online environment (Swagger UI).

Data SVP!

With the recent launch of the Data Sharing Valorisation Programme (Data SVP!), the Netherlands is investing in scalable data spaces. The programme supports initiatives that are ready to grow and helps them strengthen adoption, maturity and interoperability.

By focusing on real use cases with real value, Data SVP! stimulates the development of data spaces that are not only technically robust but also economically and socially relevant. This aligns seamlessly with the broader European ambition to build sovereign, future-proof data ecosystems.

< photo team with first prize: Ines Martinez Bustamante, Ioannis Tolios, Ivo van Dijck and Giulia Biagioni / CoE-DSC >

Driving force

In addition, the Netherlands is exploring the possibility of appointing a national organisation as a Gaia-X Digital Clearing House. This role is crucial: it acts as an independent party that verifies whether services comply with Gaia-X rules. A Dutch Clearing House would significantly accelerate and strengthen the adoption of sovereign cloud solutions in the Netherlands.

In short, the Dutch Gaia-X Hub is clearly moving from vision to realisation. Through technological innovation, national and international collaboration, and a strong focus on high-value use cases, the Netherlands is becoming a driving force in European cloud sovereignty.

< photo presentation Giulia Biagioni / CoE-DSC >

4.3.1 EMPOWER-X

EMPOWER-X in DS4PED Rubí: trusted energy data for renewable EV charging

Paco Conde, Co-Founder & **Jose David Doria**, Chief Operations Officer & **Gio Dal Mas**, Project Manager at Zertifier, Catalonia

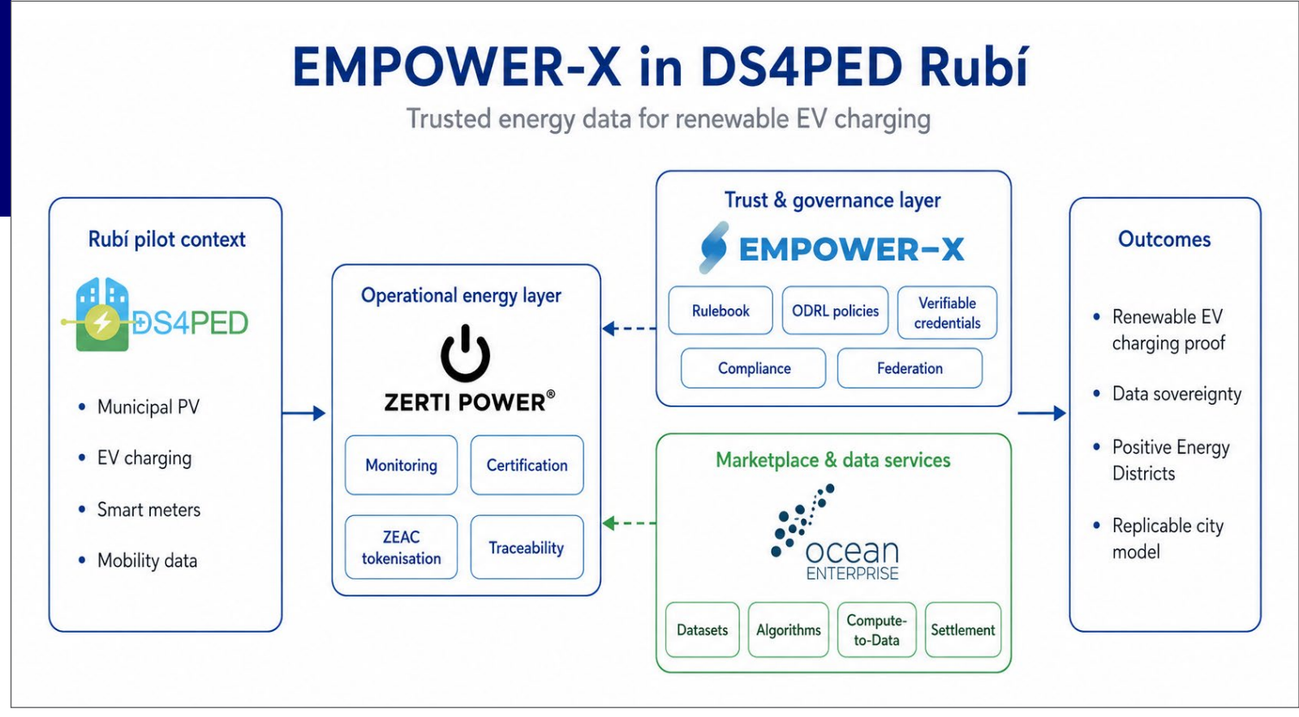


IMAGE 2 - EMPOWER-X in DS4PED Rubí architecture diagram

Energy data spaces become relevant when they help cities solve operational problems. EMPOWER-X, recently recognised as a Gaia-X Lighthouse Ecosystem, applies this approach to the DS4PED pilot in Rubí, where trusted data sharing is used to certify renewable energy use in electric mobility and support the deployment of Positive Energy Districts.

Rubí provides a strong municipal testbed. The city has 31 photovoltaic installations, with 1.5 MWp of installed capacity, and 15 EV charging points. The challenge is not only to produce local solar energy, but to prove when and how this energy is used. Solar generation and charging demand do not always match, especially at night. The Rubí pilot therefore links municipal PV production, EV charging consumption, smart-meter data and mobility services through a traceability layer that can verify the renewable origin of charging events.

EMPOWER-X combines four functional layers. The Rubí pilot context provides the operational datasets: municipal PV, EV charging, smart meters and mobility data. ZertiPower acts as the operational energy layer, supporting monitoring, certification, ZEAC tokenisation and traceability. The trust and governance layer, aligned with Gaia-X principles, defines the rulebook, access conditions, ODRL-based policies, Verifiable Credentials, compliance and federation. The marketplace and data services layer, supported by Ocean Enterprise Collective, enables publication, discovery and controlled use of datasets, algorithms and Compute-to-Data services.

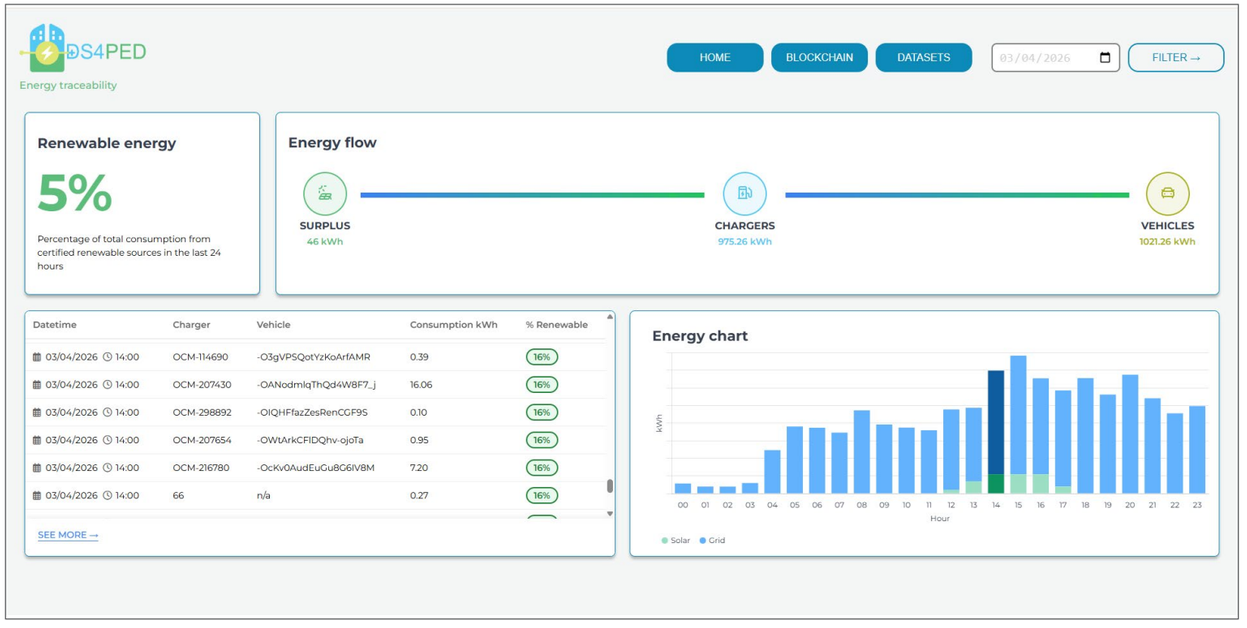


IMAGE 1- DS4PED Rubí energy traceability dashboard: certified renewable energy, surplus solar production, EV charging consumption and hourly solar/grid contribution.

A key element is the tokenisation of surplus solar production into ZEAC tokens, linked to digital guarantees of renewable origin. These tokens can be used when direct solar generation is not available, helping the city maintain a verifiable renewable-energy balance for EV charging. Instead of relying on generic green claims, the system connects energy flows, data products and governance rules into auditable digital evidence.

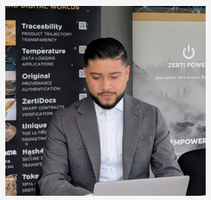
Ocean Enterprise Collective strengthens this model by adding a data-service marketplace layer. Energy and mobility datasets, algorithms and Compute-to-Data services can be published, discovered and accessed under defined policies. This is important for public infrastructure, where

data may be sensitive, commercially valuable or linked to citizens, and where controlled execution of algorithms can be preferable to moving raw datasets.

The lesson from Rubí is that Gaia-X principles are most useful when connected to execution. A rulebook defines who can access a data product, for which purpose, under which conditions and with which audit trail. Machine-readable policies and compliance services can then enforce those rules in daily operation.

For cities, EMPOWER-X offers a replicable path to Positive Energy Districts: renewable energy can be monitored, certified, shared and verified within a sovereign data space. For Gaia-X, the Rubí pilot shows how trust, interoperability and data sovereignty can become concrete municipal infrastructure.

Paco Conde, Co-Founder at Zertifier, Catalonia

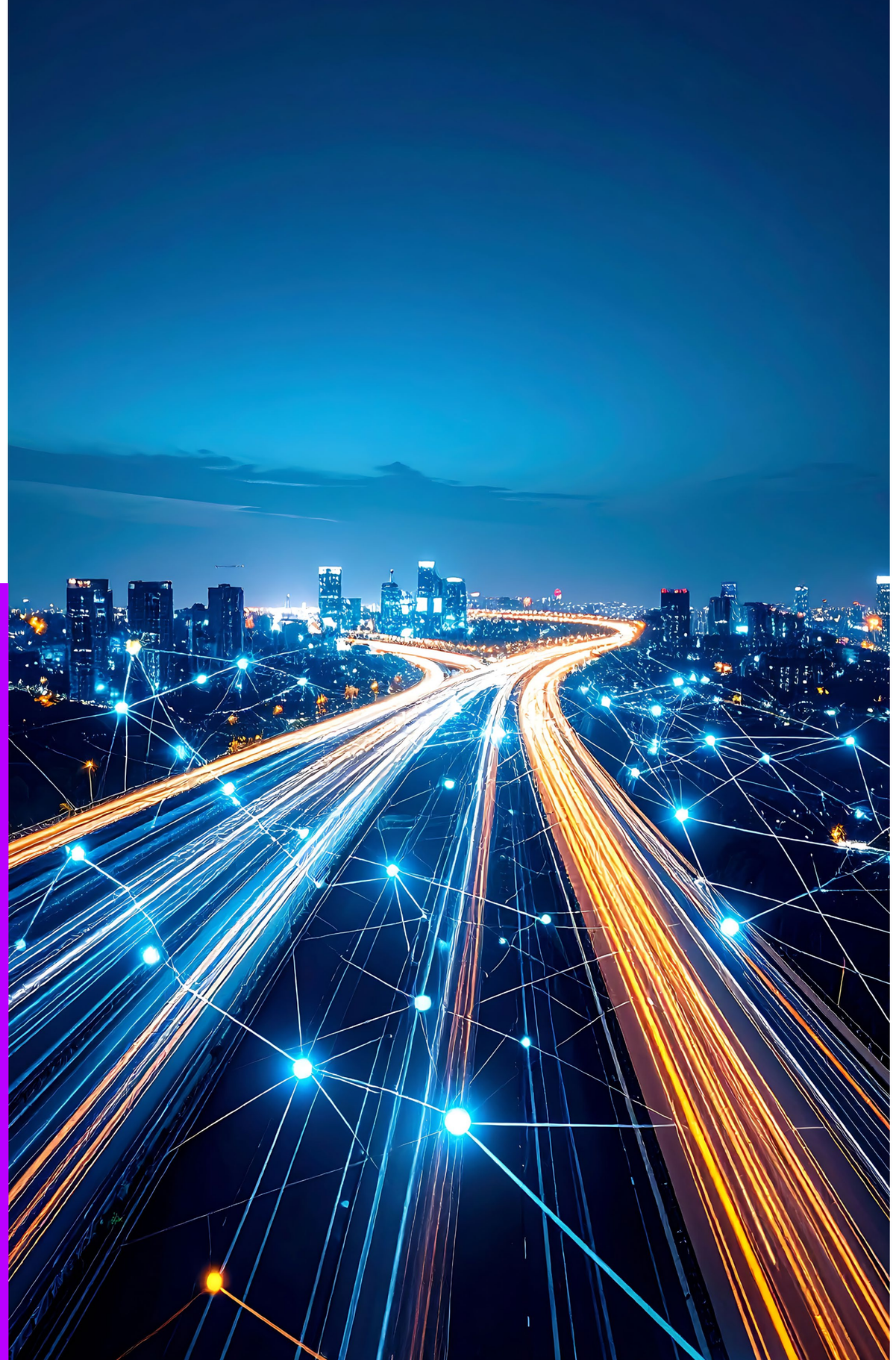


Jose David Doria, COO at Zertifier, Catalonia

Gio Dal Mas, Project Manager at Zertifier, Catalonia

Conflict of interest statement

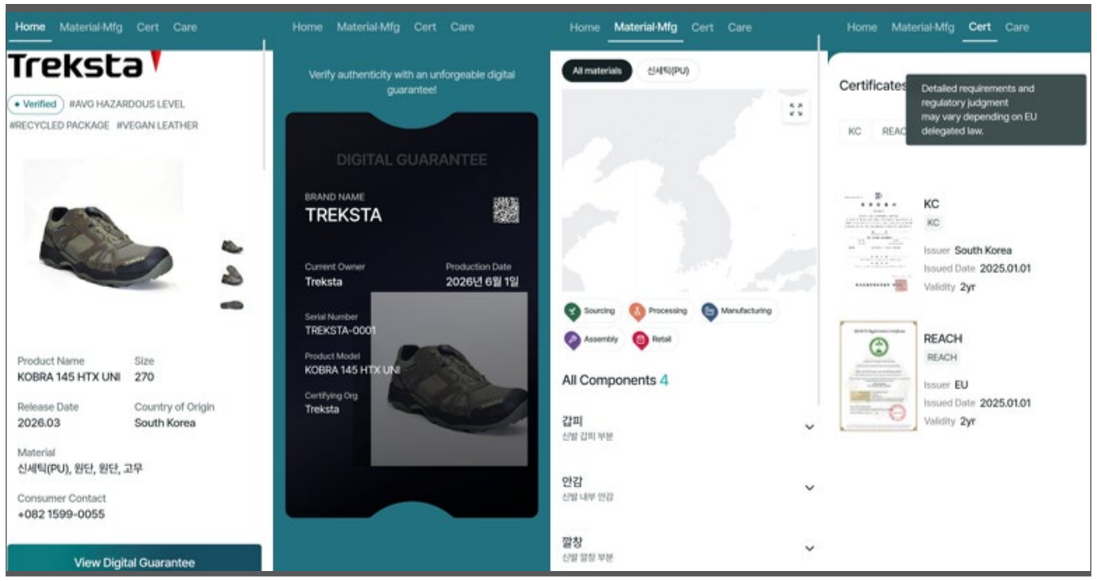
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in the submitted work. The current submission presents original work attributed to the authors cited in this article and has not been previously published or sponsored to be published in any other publication other than the Gaia-X Magazine.



4.3.2 Shoes-X

Shoes-X Expands Trusted Data Spaces from Europe to Asia Through Gaia-X Innovation

Myungkwan Shin, Chief Executive Officer at Circular solution



Shoes-X Expands Trusted Data Spaces for the Global Footwear Industry

As a Gaia-X Endorsed Lighthouse Project, Shoes-X continues to drive digital transformation in the footwear industry by building a trusted, interoperable, and sovereign data ecosystem connecting manufacturers, brands, suppliers, and service providers across international markets.

Over the past months, Shoes-X has achieved three major milestones that demonstrate the growing adoption of Gaia-X principles in Asia and strengthen collaboration between European and Asian industrial ecosystems.

Strategic Partnership for Sustainable Footwear Innovation

A key achievement was the signing of a Memorandum of Understanding (MOU) between Circular Solution and the Footwear & Fashion Promotion Division of Busan Techno Park, Korea's leading footwear industry support organisation. The partnership aims to help footwear companies respond to increasing sustainability requirements, Digital Product Passport (DPP) initiatives, and global regulatory demands.

Through this collaboration, Shoes-X provides trusted digital infrastructure to support secure data sharing, sustainability reporting, and supply chain transparency. The initiative helps footwear manufacturers improve competitiveness while preparing for emerging international standards and compliance requirements.

Youngho Kang (left), Director, Footwear & Fashion Promotion Division, Busan Technopark / MyungKwan Shin (right), CEO, Circular Solution

Establishing a Gaia-X Digital Clearing House for Asia

Shoes-X has expanded its role by providing Digital Clearing House services that enable Korean and Asian companies to participate in trusted data spaces based on Gaia-X principles.

Through this capability, organisations can obtain and manage Gaia-X-compatible digital credentials, verify identities, and onboard into secure data-sharing environments. This creates a practical pathway for Asian businesses to connect with European and global data ecosystems while maintaining control over their data and digital assets.

By lowering barriers to participation and supporting trusted cross-border collaboration, Shoes-X contributes to the broader vision of federated and interoperable data spaces that support transparency, innovation, and digital sovereignty.

Award-Winning Innovation in Trusted Data Exchange

A major milestone was the recognition of Circular Solution's OID4VC-based credential solution at the Gaia-X Tech-X Hackathon, where it received the second prize among competing European data space innovations.

The award recognised the practical implementation of OpenID for Verifiable Credentials (OID4VC) and Eclipse Dataspace Components (EDC) technologies to support trusted data exchange within the footwear industry. The solution enables participants to issue, verify, and exchange digital credentials while maintaining data sovereignty, access control, and policy compliance.

Integrated into the Shoes-X ecosystem, this capability provides a foundation for trusted business interactions, Digital Product Passport initiatives, supply chain traceability, and secure cross-border collaboration. The recognition demonstrates how Gaia-X technologies can be successfully applied to real industrial use cases

Bowen Chong (left centre), Research Engineer, Circular Solution / MyungKwan Shin (right centre), CEO, Circular Solution

and validates Shoes-X as a leading example of data space implementation beyond Europe.

Looking Ahead

The footwear industry is facing increasing demands for sustainability, traceability, and digital collaboration. Shoes-X is addressing these challenges by creating a trusted data space that enables secure information exchange across the entire value chain.

Through strategic partnerships, Digital Clearing House services, and award-winning trusted data exchange technologies, Shoes-X is helping shape the future of digital ecosystems in the footwear sector. As adoption continues to grow, the project remains committed to extending Gaia-X principles beyond Europe and fostering a globally connected, trusted, and sovereign data economy.

CIRCULAR SOLUTION

Partners

제단법인 부산테크노파크 BUSAN TECHNOPARK

Treksta

JC MEDI

TUBLOCK THE FIRST STEP TO A HAPPY LIFE

EST BSL MMX BAKE-SOLE

CORE OF ALCHEMY

4.3.3 **Dataspace4Health**

Dataspace4Health: a Gaia-X Lighthouse project moving from reference architecture to working components

Seyed Ziaeddin Alborzi, PhD, Senior Data & AI Go to Market at NTT DATA

Dataspace4Health is a Luxembourg-based Gaia-X Lighthouse project for health, moving from reference architecture to concrete, testable open-source components for trusted health data sharing. It provides technical rails for governed, sovereign and traceable data exchange, designed to support EHDS-aligned secondary use under the appropriate governance authorities, not to centralise data or replace existing health-governance authorities.

The project connects healthcare and research actors around a federated model: data holders keep control, data users discover and request datasets through common mechanisms, and exchange is framed by identity, metadata, policy, contract and traceability capabilities. This is being applied to two high-value scenarios, diabetes digital twin and precision oncology, where fragmented data across hospitals and research institutions slows innovation.

A key milestone has been the demonstrated end-to-end Eclipse Dataspace Connector flow between HRS (Hôpitaux Robert Schuman) as data holder and LIH (Luxembourg Institute of Health) as data user, using Federator-based catalogue capabilities, policy and contract definition, negotiation, and data transfer through the participant dashboard. Alongside this, the pilot includes deployed connector instances for HRS and LIH, Federator-supported onboarding, and HealthDCAT-AP metadata capture.

Onboarding and trust establishment have also advanced. Dataspace4Health uses a Gaia-X Danube-based credential approach in which the Federator generates and signs LegalPerson Verifiable Credentials. Registration numbers are checked through the Gaia-X Notary, and credentials are used inside the consortium trust model. They extend the LegalPerson model with Dataspace4Health-specific onboarding and connector claims such as participant DID, DSP endpoint, supported protocols, jurisdiction and roles.

DATASPACE 4HEALTH LUXEMBOURG

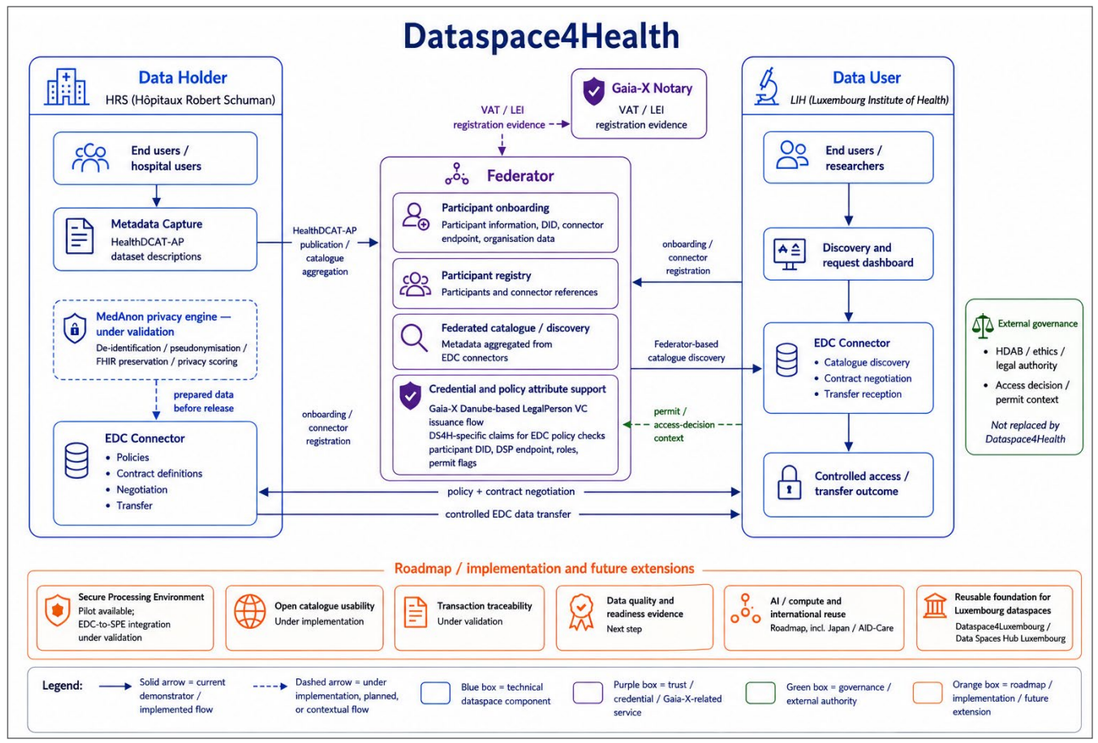
A Metadata Capture component supports HealthDCAT-AP-based dataset descriptions, while a synchronisation service updates EDC assets from published metadata, linking rich health metadata to exchange and reducing manual work for data holders.

For data preparation, Dataspace4Health is complemented by MedAnon, a rule-driven privacy engine under development. It is designed to support de-identification, pseudonymisation, clinical text protection, FHIR structure preservation, privacy scoring and auditable release decisions, bridging privacy requirements and technical controls before reuse.

A Secure Processing Environment pilot is available as a trusted processing capability, while direct EDC-to-SPE integration is still under implementation; the project is not yet claiming a fully operational chain but is building toward controlled delivery into it.

Beyond the health pilot, Dataspace4Health also creates reusable foundations for Luxembourg's wider dataspace community. The same building blocks can support other verticals under the Dataspace4Luxembourg direction and contribute to the Data Spaces Hub Luxembourg community. The project also prepares the ground for international health data exchange, including future collaboration with Japan through Artificial Intelligence for neurodegenerative diseases Care (AID-Care) project.

Next steps focus on hardening the operational chain: EDC-to-SPE integration, open catalogue usability, transaction logging and audit capabilities, data quality and readiness evidence, and stronger alignment with EHDS secondary-use workflows. Dataspace4Health demonstrates how Gaia-X health-dataspace principles become practical, trusted and interoperable components.



05

EVENTS

In this era of rapid digital transformation, Gaia-X has emerged as a driving force, aiming to shape the future of data infrastructure and cloud services in Europe and beyond. With our focus on data sovereignty, interoperability, and trustworthiness, Gaia-X has garnered attention from industry leaders, policymakers, and technology enthusiasts alike. Through this dedicated section, we aim to provide you with comprehensive insights into Gaia-X events, keeping you informed about the latest developments, key announcements, and upcoming events.

05

PAST EVENTS

Tech-X & Hackathon #9 Athens
Gaia-X Sets Practical Interoperability in Motion

Athens became a focal point for Europe's data ecosystem ambitions on 28–29 May 2026, as Gaia-X, together with Gaia-X Hub Greece operated by the Laboratory for Manufacturing Systems & Automation (LMS), hosted Tech-X and Hackathon #9. The event highlighted Gaia-X's evolution from a broad architectural vision toward enabling practical cross-ecosystem interoperability.

One of the highlights of the event was the introduction of the Gaia-X Loire Participant Credential Wizard by the Gaia-X Lab Team, a new tool designed to simplify participant onboarding in the Gaia-X ecosystem by enabling the creation and signing of Verifiable Credentials compliant with the Gaia-X Trust Framework.

The event also demonstrated the practical implementation of Gaia-X 3.0 "Danube" across several key dimensions:

Ecosystem level: Participants heard directly from full-fledged data spaces and ecosystems as they presented requirements and technologies and explained why these could only be fulfilled by Danube's features, like the IMXC (International Manufacturing-X Council) "federated trust" use case, which implements trust between different ecosystems and is supported by the Danube Gaia-X Core Engine and the Gaia-X Meta-Registry. MYRTUS, a project focused on orchestrating the cloud–fog–edge continuum securely and sustainably, showcased the **MYRTUS–Gaia-X Danube** compliance framework live, illustrating how the project uses Gaia-X Danube to verify whether a partner is eligible to join a MYRTUS cluster, using Gaia-X Verifiable Presentations and Verifiable Credentials.

Technical level: Participants learned how to use **'Bring Your Own Rules' (BYOR)** concept made easy, using OPA and Rego with Gaia-X Danube, and what the design decisions and open problems are, plugging a Multi-Ecosystem Federation into the Gaia-X Meta-Registry.

Connector level: Danube is all about trust. Various data space connector technologies that incorporated the principles defined in the latest Danube architecture document were showcased, including Eclipse Data Space Components (EDC) with OID4VC: an MVP demonstration; From Standard to Open Source Stack: Implementing Trusted Data Transactions with the Gaia-X Framework and the Data Transfer Agent. The presentation examined how to implement Trusted Data Transactions with the Gaia-X Framework and an open-source implementation example of a Data Transfer Agent.

Compliance DIY Workshop: This hands-on session enabled participants to bring their own BYOR requirements and receive direct support from the Gaia-X Lab team in implementing them on the Gaia-X 3.0 Danube platform.

"From a technology perspective, Tech-X and our overfull Hackathon #9 showed that Gaia-X is entering a more mature implementation phase," said **Christoph Strnadl**, Chief Technology Officer of Gaia-X. *"Danube is important because it makes compliance execution more modular and extensible, while BYOR is imperative because real ecosystems need to combine rules from different domains and custodians. That is the difference between a framework that is described and a framework that is actually automated and operationalisable."*

Hackathon #9 reinforced that implementation focus. The list of hacks included work on reusable compliance rules, policy- and credential-aware invocation on Gaia-X Danube, agentic automation of trust exchange, and AI-related approaches to sustainable cloud architectures.

Winners were announced on 29 May, with prizes of 5,000 euros for first place, 3,000 euros for second place, and 1,500 euros for third place.

1st place – The Agentic Automation of Trust Exchange in Gaia-X Framework – The hack goal is to create a prototype demonstrating end-to-end agentic trust orchestration for Gaia-X service federations, showing how the Gaia-X trust framework can serve as the trust and policy backbone for AI-mediated, multi-agent service interactions.

2nd place – Selective Disclosure Cross-Jurisdiction Identity Credentials for Gaia-X – Gaia-X's notary today recognises only EU-centric identifiers (EORI, EUID, vatID, LEI, taxID), and the entire credential pipeline issues plain JWS, where every claim is either fully visible or absent. Both limitations either exclude participants from outside the EU, or force them to expose more than they need once inside.

3rd place – Policy and Credential-Aware A2A Skill Invocation on Gaia-X Danube – The Proposal to build an end-to-end demonstrator on Gaia-X 3.0 Danube that covers agent to agent (A2A) interaction, VC-based verification of the calling agent, and DUA-based authorisation of provider skills. The hack demonstrated how Gaia-X 3.0 Danube can support interoperable agents that handle conditional data utilisation across organisational boundaries.

For **Ulrich Ahle**, Chief Executive Officer of Gaia-X, the event in Athens highlighted the ecosystem's growing practicality. *"An important signal from Athens is that the Gaia-X ecosystem is developing practical tooling for different levels of maturity. Not every participant enters with the same technical resources, and that is precisely why reusable rules,*

shared components and interoperable building blocks matter so much. As a result, trust becomes automated, sovereignty becomes actionable, and Europe's digital future can be built on solid, shared foundations," he said.

Kosmas Alexopoulos, Professor at the Laboratory for Manufacturing Systems & Automation (LMS), emphasised the role of artificial intelligence in future industrial ecosystems. "The combination of GenAI and Gaia-X Data Spaces creates a new foundation for industrial intelligence: data remains sovereign, collaboration becomes trusted, and AI services can generate actionable insights across companies, factories, and value chains," he noted.

Tech-X Athens thus represented an important milestone in Gaia-X's 2026 agenda, demonstrating how governance, compliance and interoperability can be embedded into working components and tested against real use cases. The event also helped build momentum toward the Gaia-X Summit 2026 in Vienna, where the association will continue its focus on "Season 2.0 of Sovereign, Trusted AI & Data Ecosystems".

UPCOMING EVENTS

Save the Date – Gaia-X Summit 2026

Join us on 19–20 November 2026 in Vienna, Austria, for the 7th Gaia-X Summit, organised in cooperation with Gaia-X Hub Austria, operated by AIT Austrian Institute of Technology GmbH. Under the theme "Season 2.0 of Sovereign, Trusted AI & Data Ecosystems", the summit will showcase how Gaia-X is moving from foundation-building to large-scale market adoption, enabling trusted data sharing, trustworthy AI, and economically sustainable data ecosystems.

Why join us

Achieve higher levels of compliance with significantly greater efficiency, leading to measurable cost reductions. Enable greater transparency and faster decision-making by integrating the Trust Framework into operations, enabling compliance automation and supporting quicker, data-driven decisions. Unlock scalable value creation by enabling organisations to collaborate across ecosystems, making it easier to develop, scale, and monetise data products and insights within trusted networks. Low entry barriers and ease of adoption ensure the solution remains practical and cost-effective to implement and simple to use, balancing upfront investment with longer-term value realisation. Global reach and relevance are reflected in international participation from Canada, South Korea, and Japan, demonstrating applicability to global digital and supply chains beyond a purely European focus.

Acknowledgments

Special thanks to the authors, Gaia-X editorial, web and communications teams for their efforts and support to finalise this issue.

TOGETHER TOWARDS A

FEDERATED AND SECURE DATA INFRASTRUCTURE

Gaia-X MAGAZINE

June 2026 | Edition 8