

RECOMMENDATIONS TO FURTHER DEVELOP THE EU-JAPAN DIGITAL PARTNERSHIP

Introduction

The Japan Business Council in Europe (JBCE) welcomes the opportunity to contribute to the EU-Japan Tech Business Roundtable, a public-private dialogue convened ahead of the 2026 EU Japan Digital Partnership Council, and reaffirms its continued commitment to the development of the partnership. This contribution builds on the outcomes of the 2025 EU–Japan Summit, which reaffirmed the strategic importance of deepening digital and economic cooperation and called for more concrete and scalable implementation under the Digital Partnership.

The development of digital technology is not an end in itself. Its value lies in its application: providing novel solutions to complex societal challenges, propelling industrial competitiveness forward, and offering an ever-wider array of possibilities to citizens and businesses. The EU and Japan share the ambition to lead in this space, while also possessing the institutional discipline to ensure that technology will serve rather than undermine these goals. The pursuit of accountable innovation grounded in the rule of law and democratic values is a common foundation, and represents the Partnership's most distinctive and durable asset.

This paper argues that realising the full potential of the EU-Japan Digital Partnership calls for a transition from a dialogue-oriented phase to one focused on concrete, outcome-driven implementation. To this end, JBCE identifies priority areas for action, including AI, data, cybersecurity, emerging technologies such as quantum and space, as well as physical infrastructure and supply chain resilience. As this bilateral cooperation deepens, JBCE proposes moving beyond bilateral frameworks to establish the Trusted Digital Commons (TDC) as its organising principle. The TDC represents the digital implementation of 'Made with Common Values (MwCV)': a principle underpinning economic cooperation based on shared commitments to sustainability, trust, resilience, the rule of law, and human rights.

Under this framework, Data Free Flow with Trust (DFFT) — first proposed at the G20 Osaka Summit in 2019 and subsequently advanced through G7 processes, including the 2023 Hiroshima Summit, with the OECD hosting the Secretariat of the International Forum on the Governance of Data Free Flow with Trust (IAP) —has established a normative objective: data should flow freely among partners maintaining equivalent standards of trust. Yet 'trust' in DFFT remains operationally undefined. That gap is increasingly being filled by national sovereignty frameworks built on geographic criteria, an approach that fragments markets, raises costs for compliant local providers, and widens existing price asymmetries in favour of global hyperscalers, thereby increasing the risk of further concentration of critical digital infrastructure in the hands of a small number of providers.

The TDC offers a different criteria-based solution: conditional openness grounded in verifiable standards of security, governance, and interoperability, regardless of national origin. The EU–Japan digital partnership represents the natural core of this architecture, demonstrating that digital sovereignty and market scale are mutually reinforcing rather than competing objectives. With regulatory credibility, market scale, and a high-trust partnership, it is well placed to exercise leadership and to provide a foundation for the progressive participation of like-minded partners. In this context, JBCE sets out its recommendations across the following priority areas, with a view to translating political commitment into measurable outcomes in both economies and economic securities.

KEY MESSAGES

❖ **From solid plans towards concrete action**

The EU–Japan Digital Partnership has built strong political momentum since its launch in 2022. The task now is to move from ideas to outcomes measurable in investment flows, joint technology programmes, and regulatory convergence that delivers real cost reductions for businesses operating in the trusted digital sphere. As the partnership matures we are committed to playing an active role in helping both sides achieve concrete, measurable outcomes ahead of the 2026 Digital Partnership Council. A 'Made with Common Values' approach to the digital sphere with the EU and Japan at its core, will be crucial.

❖ **Scaling 'Made with Common Values' through the Trusted Digital Commons**

JBCE calls on both sides to deepen their bilateral digital cooperation on the basis of 'Made with Common Values'. JBCE proposes organising it around the TDC, a framework of conditional openness in which any qualified jurisdiction or entity that meets agreed criteria on security, governance, interoperability, and transparency may participate. By embedding neutral, interoperable technologies as the basis for trust rather than geographic origin, TDC provides a credible path toward the practical realisation of Data Free Flow with Trust and a scalable foundation for the progressive participation of like-minded partners.

❖ **Scale markets and innovation with common values**

The EU and Japan together represent over 20% of world GDP, one in every five dollars of global economic output. Integrating this market through the principles of the MwCV, both regions can create the scale necessary for trusted technologies to compete commercially without relying on protectionist measures that impose high costs. It is important to ensure that digital infrastructure is resilient across IT, OT and emerging Physical AI environments especially in society's most critical sectors such as energy, manufacturing, and public services. Operating under common values at such scale becomes a competitive advantage.

1. Strategic Context – Why New Rules Are Needed

1.1 Existing rules grow obsolete as geopolitical tensions intensify

The digital technology rulebook, from technology creation to operations across borders and underlying remedies, is no longer fit for purpose. That framework assumed that technology supply chains were commercially driven and largely trustworthy, that geopolitical rivalries would not extend to the infrastructure of everyday digital life, and that open trade would reliably produce shared prosperity. Those assumptions no longer hold.

The partial decoupling of technology supply chains, the acceleration of state-directed industrial programmes in major economies, the weaponisation of digital dependencies, and the growing concentration of critical infrastructure in the hands of a small number of actors have altered the strategic environment fundamentally. Trust-based open trade can no longer be taken for granted. It must be designed, certified, and enforced.

This is not an argument for closed markets or technological nationalism. Restricting access to the best available technology creates real costs, and supply chains built on political criteria over commercial logic are expensive and brittle. The answer to the erosion of trust is not to abandon openness, but to rebuild it above a more durable foundation: a framework of conditional openness among qualified partners who meet verifiable standards of security, governance, and interoperability.

The EU and Japan are uniquely positioned to design and lead this new approach. Both are mature democracies with deep technological capabilities, strong institutional traditions, and a shared commitment to a rules-based order. Neither can achieve at scale what both can achieve together. The EU-Japan Digital Partnership has the potential to foster the creation of the new rules architecture which the digital economy requires.

1.2 ‘Made with Common Values’ and Market Scale

The EU and Japan can take the lead on creating integrated markets among partners sharing democratic values, the rule of law, and open governance that can produce more resilient, innovative, and trustworthy outcomes than dependence on any single external actor. This principle has been consistently advanced by JBCE in dialogues with European institutions and is increasingly recognised as the organising logic of EU-Japan economic cooperation.

The EU and Japan account for over 20% of world GDP, equivalent to one-fifth of global economic output. Together, the EU and Japan can create an integrated market under conditions in which trusted technologies achieve commercial competitiveness without relying on protectionist measures. Barriers such as divergent standards, high

certification costs, fragmented procurement become tractable when addressed at the scale of a shared market built on common values. An integrated market of such scale enables both regions to attract the investment, talent, and innovation that the trusted digital sphere requires.

2. Progress to Date, Strategic Challenges, and the Way Forward

2.1. Laying the Foundations of EU–Japan Digital Cooperation

The EU–Japan Digital Partnership was signed in May 2022, during the 28th EU-Japan Summit. It was designed to advance cooperation on digital issues and foster innovation, competitiveness and a human-centric digital transformation based on common values. It covers areas including semiconductors, 5G/6G, AI, online platforms, digital identities, data governance, quantum computing and cybersecurity.

Since then, the Partnership has developed rapidly. The third Digital Partnership Council meeting, held in Tokyo in May 2025, reaffirmed the growing importance of the Partnership in the face of global geopolitical uncertainties, with both sides recognising the need to boost competitiveness and promote a values-driven approach to global digital governance. JBCE welcomes this momentum and recognises the Digital Partnership as a cornerstone of the broader EU–Japan strategic relationship. Nonetheless, political commitment must continue to translate into concrete and measurable outcomes.

2.2. Deepening Cooperation through Joint Research and Innovation

In December 2025, the European Commission and the Government of Japan successfully concluded negotiations on Japan's association to Horizon Europe, the EU's flagship research and innovation funding programme. This milestone opens a new chapter in EU–Japan cooperation in science, technology, and innovation. JBCE celebrates this development, which creates new opportunities for joint digital projects, cross-border research consortia and the co-development of emerging technologies. We encourage both parties to maximise the practical benefits of this association by facilitating participation from Japanese companies in relevant Horizon Europe funding streams.

Building on this momentum, JBCE looks forward to exploring further avenues for deepening institutional cooperation. In particular, we would welcome discussions on the possibility of Japan's association with the European High Performance Computing Joint Undertaking (EuroHPC JU), and promoting the participation of Japanese companies in opportunities under the Digital Europe Programme on initiatives that are

closely aligned with Japan's own strengths in supercomputing, semiconductors and digital infrastructure. Such engagement would further strengthen the foundation for joint innovation and keep EU–Japan cooperation in line with the rapid evolution of the digital landscape.

2.3 Towards a Shared Approach to Digital Sovereignty

Both the EU and Japan have expressed ambitions around digital sovereignty. JBCE acknowledges the legitimacy of this objective while emphasising that sovereignty strategies should remain outward-looking and compatible with trusted partners. A 'Made with Common Values' approach, characterised by supply chain cooperation with trusted partners that share values such as free trade, democracy and human-centricity, with the relationship between the EU and Japan at its core, is crucial in this regard. We call on the EU and Japan to develop a joint understanding of digital sovereignty that enables strategic autonomy without fragmenting the international digital economy, in the spirit of 'Made with Common Values'. This requires close coordination not only at the bilateral level but also with EU Member States, to ensure coherence across the full governance architecture.

This principle finds direct application in the Cloud and AI Development Act (CAIDA), currently under development in the European Commission, which represents one of the most ambitious EU legislative initiatives in the digital sphere. While JBCE supports the goal of a more resilient and competitive European cloud and AI ecosystem, the manner in which the CAIDA might be designed and implemented will have significant consequences for Japanese companies operating in Europe. We call for the CAIDA to be a driver for cloud and AI development 'with Common Values'. In particular, JBCE requests the EU to ensure that the implementation of CAIDA does not create unnecessary friction in the existing cooperative architecture with Japan. Given Japan's high standards of data protection and its track record as a trusted partner, new EU digital frameworks should be applied in a manner that reinforces, rather than complicates, ongoing bilateral digital engagement. Both sides should ensure that explicit equivalence mechanisms for trusted partners are incorporated at the drafting stage.

3. From Common Values to Collective Action

JBCE strongly supports the legitimate goals underpinning the EU and Japan's digital sovereignty ambitions, such as reducing critical dependencies, ensuring verifiable control over sensitive infrastructure, and maintaining the ability to operate essential digital functions free from external coercion. In this context, JBCE proposes a conceptual foundation for the next phase of the Partnership that translates these shared ambitions into a verifiable and scalable architecture.

3.1 DFFT and TDC: From Principle to Implementation

JBCE proposes that EU and Japan take into account the following elements in shaping the conceptual foundation of the next phase of the Partnership. The “Made with Common Values” principle implies an implementation architecture for the digital sphere in which participation is determined by verifiable criteria rather than geographic origin, and in which trust is defined on the basis of technical and legal standards rather than assumption. The Trusted Digital Commons operationalises this approach which provides the principled answer: not unilateral sovereignty, but collective digital sovereignty achieved through international cooperation among qualified partners. Its technical and governance architecture is set out in the Annex to this paper.

DFFT represents one of the most significant contributions by the EU and Japan to international digital governance. The term has been adopted at G20 level, representing a diplomatic achievement of the first order. DFFT remains the appropriate normative framework for international data governance: a universal principle, open to all, that data should flow freely among partners maintaining equivalent standards of trust. JBCE strongly supports its continued development in multilateral fora. However, the meaning of 'trust' within DFFT remains contested, and that ambiguity creates space for divergent national interpretations. The TDC represents the EU–Japan contribution to resolving that ambiguity: a concrete, criteria-based implementation in which 'trust' is given a verifiable technical and legal definition. Progress already made in the bilateral relationship, including toward mutual recognition of cybersecurity conformity assessments and data space interoperability, provides the proof of concept.

3.2 Regulatory Convergence in Practice: Key Instruments

The TDC points toward a clear long-term direction for EU-Japan regulatory relations: the progressive reduction of barriers between qualified partners, with the goal of conditions that increasingly approximate national treatment within the trusted digital sphere. As a practical step toward this objective, both sides would benefit from regulatory cooperation through structured exchanges starting from the drafting stage of new legislation, enabling mutual recognition of certification schemes to extend, over

time, to implementation-level requirements. JBCE would welcome the establishment of such an exchange mechanism as a foundation for future policy alignment.

This direction of travel has direct implications for three current legislative instruments:

Cloud and AI Development Act

The CAIDA should be designed to strengthen EU-Japan digital cooperation, not complicate it. Sovereignty requirements under CAIDA should assess verifiable technical and governance criteria, and should not treat qualified partners with common values as generic third-country risks. Both sides should ensure that explicit equivalence mechanisms for trusted partners are incorporated at the drafting stage.

Cybersecurity Act II

The Cybersecurity Act II (CSA2) introduces a framework for managing ICT supply chain risks, including the designation of high-risk suppliers based on non-technical criteria such as third-country legal exposure, ownership structure, and governance. JBCE strongly supports this risk-based approach. However, the application of high-risk designations should be consistent with the TDC framework's verifiable governance, transparent ownership, and enforceable safeguards, and should not be undermined by restrictive measures designed for genuinely high-risk actors. The CSA2 could be seen as a concrete implementation of the TDC's verifiable assurance requirements. Once adopted, the Regulation's enforcement should accelerate trusted partner integration, not impede it.

Digital Platform Regulations

Cooperation between authorities responsible for the EU Digital Services Act, Digital Markets Act, and Japan's Information Distribution Platform Act and Mobile Software Competition Act should extend beyond exchanges on policy design to encompass enforcement practices. Businesses need consistent, predictable rules across both markets. In particular, the weight and enforcement of rules governing borderless digital markets can be strengthened through coordinated initiatives between jurisdictions. Both sides should ensure that existing cooperation arrangements are operationalised through regular information exchange and provide possibilities for joint enforcement, at the level of day-to-day regulatory application.

3.3 The Right to Access AI

As AI and digital infrastructure become fundamental to education, economic participation, healthcare, and civic life, access to trustworthy AI will increasingly determine what is possible for individuals, communities and economies.

Openness at the inter-governmental level must translate into meaningful access at the human level.

Investment in digital skills, education, and inclusive infrastructure is not merely social policy, as it is the precondition for a sustainable innovation cycle. Inclusivity can ensure future competitiveness, by fostering the digital-native individuals that will generate further innovation, thereby guaranteeing the next-generation talent base.

JBCE emphasises that unequal access to AI and related digital capabilities may increasingly shape competitiveness gaps across economies and industries. Ensuring broad, trusted access through international cooperation, including the EU–Japan Partnership, is therefore an important policy consideration. JBCE does not prescribe outcomes; it invites both sides to begin a constructive dialogue aimed at identifying concrete areas for cooperation.

4. Concrete Next Step to Deepen the Partnership

4.1 AI - Accelerating AI Adoption

Both the European AI Strategy, including the AI Act and the European approach to excellence and trust in AI, and Japan's AI Strategy and Basic Act on the Promotion of AI provide complementary frameworks for advancing safe, trustworthy, and competitive AI development.

A structured AI sandbox framework

Building on its continuous engagement, JBCE has consistently advocated for the implementation of more joint pilot projects, particularly in the domain of AI for the public sector and advanced manufacturing.

To support the scaling of such initiatives, a structured sandbox framework could serve as one practical mechanism, enabling real-world testing of AI solutions in a controlled environment, with results and learnings shared broadly beyond direct participants to maximise impact and foster wider adoption across both markets.

More specifically, we look forward to the establishment of sandboxes that accelerate the practical deployment of AI at scale in areas such as:

- **Genomics AI:** Advanced graph AI for integrating genetic and clinical data to enable precise diagnosis and personalised treatment.
- **Policy Twin:** AI simulation of public policy impacts — including health, tax and urban planning — to support effective and fair data-driven governance.

- **Causal AI:** Identifying true causal drivers in complex industrial and public infrastructure data for process optimisation, quality improvement and efficiency gains.
- **AI Trust Technologies:** Secure, privacy-preserving AI infrastructure for sensitive applications, ensuring data sovereignty and safe AI agent communication.

Joint programmes in Physical AI

JBCE calls for the establishment of joint programmes in Physical AI, understood as the application of AI to autonomous systems, robotics, and automated manufacturing. Physical AI enables a fundamental reallocation of human labour: by automating routine physical tasks, it frees individuals to focus on distinctly human forms of value creation in areas such as design, care, innovation, and adjudication. For the EU and Japan, both facing demographic challenges, including population decline and ageing societies, Physical AI represents a strategic response to one of the most pressing sustainable development challenges of the coming decades. It can enable the creation of an advanced industrial model that is human-centred and resilient, and can be leveraged as an exportable asset.

AI Gigafactories and the Infrastructure of AI Leadership

Equitable access to AI infrastructure as a prerequisite for inclusive and competitive digital economies makes EU-Japan cooperation in this domain both timely and strategically significant. AI Gigafactories are strategically important, in that they bring together semiconductors, high-performance computing, energy management systems, and, increasingly, quantum computing capabilities.

The EU and Japan bring complementary strengths: Japan's leadership in next-generation semiconductors, energy-efficient hardware, precision manufacturing, HPC infrastructure and growing quantum research ecosystem create a natural basis for joint development. Ensuring that AI Gigafactories are built on trusted, interoperable, and energy-efficient infrastructure, rather than on components sourced from high-risk actors, is a concrete test of whether strategic autonomy can be achieved without sacrificing openness or competitiveness. JBCE encourages both sides to include AI compute infrastructure and its physical dependencies as a formal agenda item in the next phase of the Digital Partnership.

4.2 Data – Reclaiming Strategic Control

Data is the foundational resource of the digital economy: the raw material from which AI capabilities, industrial intelligence, and new services are built. Control over data

where it is generated, stored, processed, and governed is therefore a strategic question of the first order. The EU and Japan should establish the conditions under which data generated in the physical world such as factories, hospitals, cities, and supply chains is captured, curated, and made available in ways that serve the prosperity of the TDC rather than concentrating value in the hands of any single actor.

The EU's model of sectoral data spaces (Common European Data Spaces in manufacturing, health, mobility, agriculture, and beyond) represents a significant institutional innovation for managing data at scale in a trusted environment. JBCE calls for the extension of this model to the EU-Japan partnership: joint data labs and interoperable data spaces that generate, curate, and govern Physical world data, providing the data infrastructure on which next-generation AI systems can be trained and deployed in ways that serve the common interest.

Data Free Flow with Trust

JBCE reaffirms its strong support for the DFFT initiative, which the EU and Japan have championed in multilateral fora. DFFT is based on the concept of “promoting the international free flow of data to solve business and social issues across borders while ensuring trust in privacy, security and intellectual property rights.” However, there is no common understanding of what trust means in DFFT. Hence, work needs to be done to ensure further alignment on this crucial element. The EU and Japan should lead the international discussions by engaging with the industry and agreeing on the elements and concepts of trust necessary for the realisation of the DFFT.

Data sovereignty and international data flows

At the Third Meeting of the EU–Japan Digital Partnership Council held in Tokyo in May 2025, both sides began exchanges towards a possible joint working group to facilitate practical discussions on improved data sharing, including interoperability between common European data spaces and Japanese data spaces, for example, in the automotive sector.

JBCE strongly supports this initiative and encourages both parties to accelerate this work, ensuring that frameworks for cross-border data transfer remain open and predictable for business. To that end, JBCE puts forward the following proposals:

- **Prioritise interoperability across sectors:** Rather than seeking full regulatory alignment, which would be both time-consuming and politically complex, both sides should identify the minimum technical and governance conditions under which EU and Japanese data spaces can exchange data seamlessly. Common European Data Spaces and Japan's data space initiatives (including the Ouranos Ecosystem, Japan's industrial data infrastructure platform) offer the

most immediate opportunities for pilot interoperability projects across automotive, healthcare, and industrial sectors. The proposed EU-Japan Data Strategy Working Group should be operationalised with industry as a formal participant.

- **Define trust in DFFT operationally:** There is currently no shared operational understanding of what 'trust' means within DFFT. The EU and Japan should lead international discussions to establish operational definitions specifying the technical, legal, and governance requirements that a partner must meet to participate in trusted data flows.
- **Clarify the treatment of cross-border data flows under CAIDA:** As the Cloud and AI Development Act takes shape, JBCE urges the Commission to ensure the provisions on highly secure cloud infrastructure do not inadvertently restrict data flows with partners such as Japan. Explicit carve-outs or equivalence mechanisms for trusted partners should be considered at the drafting stage.
- **A clear framework for personal and non-personal data:** Personal data flows are governed by the General Data Protection Regulation and the EU adequacy framework. Non-personal data flows, including industrial and machine-generated data, are governed by the EU Data Act and Japan's forthcoming comprehensive data utilisation framework. JBCE welcomes the extension of the adequacy decision to academia and research and urges continued progress toward a comprehensive framework covering the public sector. For non-personal data, both sides should develop compatible governance frameworks that enable cross-border industrial data flows while preserving sovereign decision-making. It drives the next phase of data-driven innovation, which builds on trusted interoperability, secure data sharing environments, and predictable regulatory conditions for businesses operating across jurisdictions.

4.3 Cybersecurity

Cyber Resilience Act

The Cyber Resilience Act (CRA) entered into force on 10 December 2024 and will apply in full from 11 December 2027. The CRA introduces cybersecurity requirements for companies placing digital products on the EU market.

However, given the broad scope of products covered, manufacturers, including many Japanese companies operating in Europe, are still working to fully understand their obligations in practice. While the recent publication of guidance is a welcome step, additional practical clarity would be beneficial to help companies implement the CRA effectively and maintain their competitiveness. In this context, a structured regulatory dialogue between EU and Japanese authorities on CRA implementation would reduce

duplicative compliance burdens and ensure that internationally aligned approaches are reflected in the standardisation process. Progress toward mutual recognition of Internet of Things (IoT) and Operational Technology (OT) security conformity assessments between the CRA framework and Japan's JC-STAR scheme should be prioritised. Both sides should also deepen cooperation on Software Bill of Materials standards, coordinated vulnerability disclosure, and cross-border incident response for critical infrastructure.

Mutual recognition in IoT security

The risk of cybersecurity incidents exists throughout our society, which increasingly relies on a wide range of IoT devices. Such incidents can significantly disrupt the functioning of the digital infrastructure that is an integral part of our daily lives. Preventive measures are therefore crucial, especially in the current context of geopolitical instability and economic security concerns. In the digital world, where borders no longer exist, we expect governments to lead global discussions on combating cybersecurity risks and to implement measures such as promoting international standards, enhancing cross-border threat intelligence sharing, and fostering public-private partnerships, all while balancing innovation with competitiveness.

Both the EU's NIS2 Directive and Japan's equivalent frameworks for the protection of critical infrastructure, including the Economic Security Promotion Act and relevant cybersecurity legislation, recognise that OT security in critical infrastructure sectors is a national security imperative. In an era of geopolitical instability, the resilience of industrial control systems in energy, transport, water, and manufacturing is as strategically significant as the security of information systems. The EU-Japan Digital Partnership must embed IT/OT security as a core requirement for participation, not only in data governance but in the physical resilience of the infrastructure on which digital services depend.

4.4 Emerging Technologies

Japan's association with Horizon Europe opens a new phase of EU-Japan research collaboration. JBCE calls for its rapid operationalisation, including for sensitive and dual-use research domains where Japanese participation has previously been limited. Investment in the following areas represents the highest priority for joint technology development.

Quantum computing and communications

The Q-Neko quantum-HPC hybrid project¹ marks a first concrete outcome of EU-Japan quantum cooperation. Joint programmes should expand to quantum communications, quantum sensing, and industrial applications in materials discovery and optimisation. Both sides should clarify the conditions for Japanese participation in sensitive quantum research within Horizon Europe².

Beyond this, Japan's potential association with the EuroHPC JU would represent a further meaningful step by providing a concrete institutional framework through which both sides could deepen collaboration in quantum computing and accelerate the development of hybrid quantum-HPC applications at scale.

6G and next-generation networks

6G research cooperation should explicitly target standardisation outcomes, ensuring that joint R&D translates into influence over ETSI, 3GPP, and ITU processes³. Open RAN architecture cooperation should be deepened, reflecting shared values on network security and supplier diversity.

The convergence of AI and telecommunications, particularly AI-native 6G architecture and AI-RAN, represents a domain of direct strategic relevance for both EU and Japanese industrial leaders. Both sides should deepen cooperation on open, interoperable telecommunications infrastructure: network architectures in which trust is verifiable, suppliers are diversified, and no single actor holds systemic leverage.

Data centres and AI compute infrastructure

AI capabilities are constrained by compute availability. Cooperation on energy-efficient data centre design, location strategy relative to renewable energy sources, and security standards, including TDC certification requirements, should be included explicitly in the partnership's infrastructure agenda.

Space

Space-based infrastructure, such as satellite communications, earth observation, and positioning systems, is increasingly integral to economic continuity and security. The

¹ [Q-Neko project \(EU-Japan quantum-HPC\)](#)

² [EU-Japan quantum cooperation / Horizon Europe](#)

³ [ETSI : EU-Japan standards cooperation \(6G/AI/quantum\)](#)

5 May 2026

partnership should include space connectivity as a formal topic, with attention to infrastructure resilience and international spectrum governance.

4.5 Physical Infrastructure and Supply Chain Resilience

Digital technology rests on physical foundations: the energy that powers computation, the semiconductors that perform it, the raw materials that compose them, and the cables and networks that carry the results. Securing this physical infrastructure, through diversification, redundancy, and deliberate reduction of single points of failure rather than autarky, is important for a durable framework. The EU and Japan are uniquely positioned to lead this effort.

Semiconductors

The EU-Japan Semiconductor Early Warning Mechanism — established to enable advance notification of supply disruptions across the bilateral semiconductor supply chain — should be operationalised actively and extended to cover a broader range of critical components. Collaborative R&D, including through the EU Jasmine project⁴, should address the full value chain from materials and equipment to advanced packaging.

Submarine cables

Arctic routing between the EU and Japan would add critical resilience to bilateral data flows. Both sides should clarify frameworks for public support where market conditions do not yet justify private investment and establish common security standards for cable landing stations.

Energy infrastructure

The energy demands of digital infrastructure (data centres, semiconductor fabrication, communications networks) are growing rapidly. Energy supply security is a prerequisite for digital sovereignty. The partnership should address this explicitly, including through cooperation on grid resilience, renewable energy integration, and the green-digital transition.

Critical raw materials

The EU and Japan should coordinate sourcing strategies for minerals essential to semiconductors, batteries, and communications equipment, working with other like-minded partner countries to develop transparent, diversified sourcing frameworks.

⁴ [JASMINE](#)

5. Conclusion – EU-Japan Digital Partnership as the Foundation for Shared Prosperity

Four years of dialogue under the EU-Japan Digital Partnership have built a strong foundation for digital cooperation across AI, data, cybersecurity and emerging technologies. The task now is to make those frameworks produce results that are visible in the trusted digital sphere: in the technologies built jointly, the data that flows freely between qualified partners, the infrastructure that is resilient because it is diversified, and the businesses that invest because the rules are predictable and grounded in common values.

The central tension this agenda must navigate is between strategic autonomy and cost competitiveness. The 'Made with Common Values' approach addresses this directly: by embedding trust in neutral, interoperable technologies rather than in geographic origin, it enables the best-available technology to be used. This is conditional openness at scale. It is the most commercially efficient path to digital sovereignty, because it leverages the combined scale of the partner ecosystem rather than requiring each participant to achieve self-sufficiency alone.

The EU and Japan possess the necessary foundations: complementary industrial strengths, shared institutional values, deep research capabilities, and a framework for integrating these assets at a scale that neither can achieve independently. Contributing to over 20% of world GDP and sharing common values are not small advantages. They are the basis for a trusted digital sphere that can set global standards, attract global talent, and demonstrate that accountable innovation is also competitive innovation.

The private sector stands ready to be a substantive partner in building this shared digital architecture, not as a stakeholder to be managed, but as the primary vehicle through which 'Made with Common Values' is translated from principle into the products, services, and infrastructure on which shared prosperity depends.

ABOUT JBCE

Founded in 1999, the Japan Business Council in Europe (JBCE) is a leading European organisation representing the interests of over 110 multinational companies of Japanese parentage active in Europe. Our members operate across a wide range of sectors, including information and communication technology, electronics, chemicals, automotive, machinery, wholesale trade, precision instruments, pharmaceuticals, textiles, and glass products.

For more information: <https://www.jbce.org/> / E-mail: sakai@jbce.org

EU Transparency Register: [68368571120-55](#)

ANNEX: THE TRUSTED DIGITAL COMMONS

What it is

The Trusted Digital Commons (TDC) is a **jointly governed architecture** through which the EU and Japan (and any partner that meets agreed criteria) establish verifiable conditions for trusted digital cooperation. It is not a political declaration, a trade agreement, or a new regulatory regime. It is the operational mechanism that translates existing principles into technically enforceable conditions.

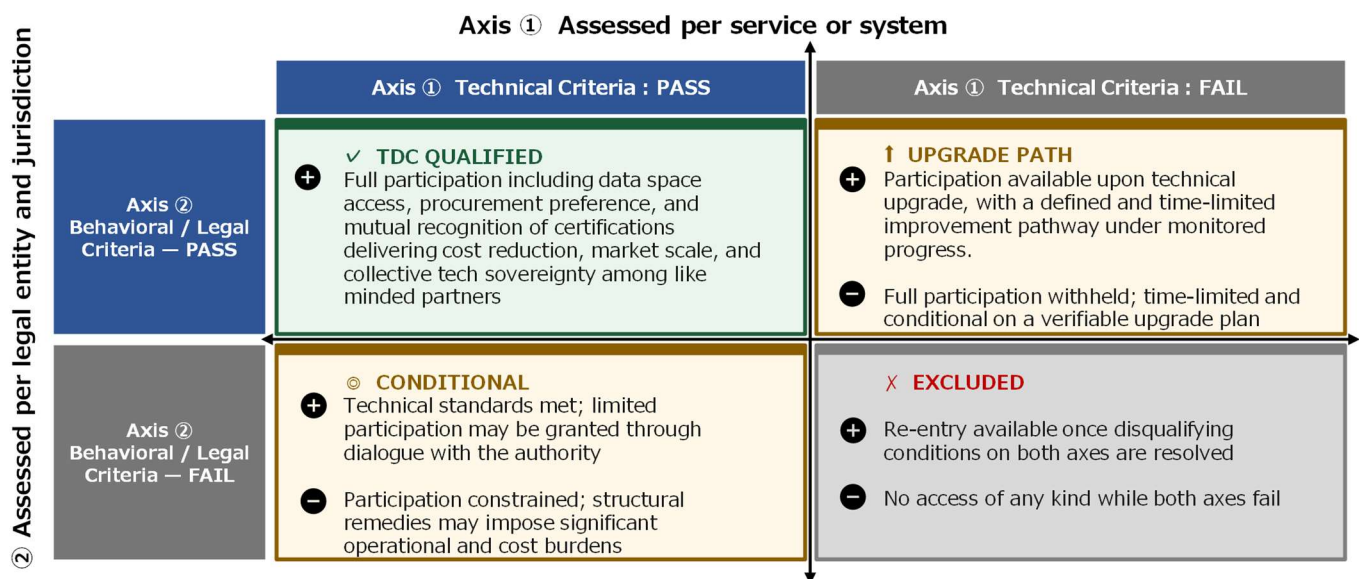
The word **Commons** is deliberate. A commons is not an open space accessible to all, but a shared resource governed by, and for the benefit of, a defined community of participants bound by the same rules and bear the same obligations. TDC is a digital commons in exactly this sense: *open to any qualified partners only, based on agreed criteria rather than origin..* Entry is determined by criteria, not by origin.

Rather than replacing the Data Free Flow with Trust (DFFT) principle or the Made with Common Values (MwCV) framework, TDC operationalises 'MwCV' through enforceable technical and governance conditions in the digital sphere.

How trust is defined: the two axes

TDC defines trust through two independent axes applied sequentially. An actor must satisfy both. (See Figure 1)

Figure 1. Dual-Axis Matrix for the Trusted Digital Commons (TDC) Qualification



Axis ① — Objective Technical Criteria

The first axis is universal, objective, and third-party verifiable. It asks whether an actor has implemented the technical controls that make trust technically meaningful. Four elements are required: security certification equivalent to EUCS High or JC-STAR with mutual recognition of conformity assessments; data control through external key management, client-side encryption, and transparent data residency; supply chain transparency via a Software Bill of Materials and a risk-based assessment process; and auditability comprising independent third-party audit rights, structured incident reporting obligations, and annual recertification within a jointly maintained governance framework. A company of any national origin can meet these criteria on their merits. These requirements collectively ensure verifiable control over data access, system integrity, and operational transparency.

Axis ② — Behavioral and Legal Regime Criteria

The second axis concerns the legal and governance environment in which an actor operates. TDC requires that participants can credibly demonstrate the independence of their operations from external directions, including governmental or legal mandates, that would conflict with the commitments made to TDC partners, in areas such as data access, service continuity, or infrastructure control. Where the applicable legal framework imposes obligations that are incompatible with these commitments, the participant does not meet this criterion.

The assessment is structural, based on legal architecture rather than political alignment. It turns on whether that architecture is compatible with the commitments required for TDC participation. Where concerns arise, they may in some cases be addressed through structural arrangements that credibly insulate the actor's TDC-related operations from incompatible obligations, with the adequacy of any such arrangements being a matter for the competent authorities.