Grant Agreement No.: 101135632 | **Call:** HORIZON-CL4-2023-DATA-01
Topic: HORIZON-CL4-2023-DATA-01-06 | **Type of action:** HORIZON-CSA

SWOT Analysis regarding Factor 2:

FRAMEWORK CONDITIONS (policies, strategies, plans and regulations)

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the other granting authorities. Neither the European Union nor the granting authority can be held responsible for them.

Copyright notice

Project funded by the European Commission in the Horizon Europe Programme		
Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Table of contents

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

1 Context

Factor 2 "Framework Conditions" addresses the regulatory, strategic and institutional environment that shapes the development and deployment of the Cognitive Computing Continuum across the EU. Framework conditions are the foundational layer of governance encompassing EU policies and regulations, Member State coordination mechanisms, and the alignment of national strategies with European objectives, that either enable or constrain the mobilisation of technological capabilities and industry participation.

Europe's regulatory landscape in digital and technology policy is increasingly comprehensive and ambitious. Instruments such as the AI Act, Data Act, Digital Services Act, Digital Markets Act, Cybersecurity Act and Cyber Resilience Act represent the EU's commitment to establishing digital markets grounded in European values: fundamental rights protection, data privacy, fair competition, cybersecurity and sustainability. This regulatory ambition is a strategic asset, differentiating the EU in global markets and building trust among citizens and businesses. However, the complexity and fragmentation of this regulatory environment, where national implementations vary, compliance requirements overlap, and bureaucratic processes remain cumbersome, create significant operational friction.

The central challenge for framework conditions is to maintain Europe's regulatory leadership and values-based differentiation while simultaneously streamlining implementation, reducing administrative burden, and creating the unified market conditions necessary for European companies to scale and compete globally. This requires both consolidating existing regulations into more coherent frameworks and reforming institutional mechanisms to achieve faster, more agile policy-making. Without such alignment, Europe risks simultaneously over-regulating its own innovators while failing to create the market unity necessary to match the scale and competitive capacity of global competitors.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

2 STRENGTHS

2.1 Europe as a Leader in Climate Policy and Digital Sustainability

Europe has established itself as a global leader in climate policy and environmental governance, with binding commitments to carbon neutrality by 2050 and the Green Deal framework. This leadership extends into digital policy, where the EU explicitly recognises the role of digital technologies in achieving climate and sustainability objectives. The Cognitive Computing Continuum, if properly architected, can become a critical enabler of European climate goals. Cloud, edge and IoT technologies, when deployed with sustainability as a design principle, can optimise resource utilisation, reduce energy waste, improve industrial efficiency and enable circular economy models across sectors.

The EU's regulatory framework increasingly mandates energy efficiency criteria for data centres and digital infrastructure, creating a differentiated competitive advantage. European computing continuum solutions can be marketed globally as inherently more sustainable and climate-conscious than alternatives from regions with less stringent environmental standards. This is not merely a compliance advantage; it is a market differentiation opportunity that allows companies building sustainable computing solutions to compete on values and long-term risk reduction in global markets, a particularly important advantage as enterprises increasingly face shareholder and stakeholder pressure to reduce technology carbon footprints.

2.2 The AI Act as a Global Regulatory Gold Standard

The EU's AI Act represents the most comprehensive and sophisticated regulatory framework for artificial intelligence adopted by any major economic bloc. Rather than being purely restrictive, the Act balances innovation protections with rights protections by establishing a risk-based regulatory approach: high-risk AI systems face strict requirements, while lower-risk applications operate with minimal regulatory friction. This nuanced approach demonstrates that Europe can regulate innovation without strangling it.

The AI Act's promulgation as EU law applicable to any organisation deploying AI in European markets creates an extraterritorial regulatory effect. Global AI developers and service providers must increasingly adapt their systems to comply with the Act, effectively setting a global standard for trustworthy AI. The Act also includes provisions supporting SMEs and startups, recognising that regulatory burden must be calibrated to company size and capacity. Companies that design AI systems to meet the Act's standards gain access to European and globally-conscious markets while building trust with users and regulators worldwide, a particularly important advantage for the computing continuum, which increasingly incorporates AI-driven decision-making at the edge and cloud layers. The regulatory credibility this provides allows European companies to compete from a position of inherent compliance rather than post-hoc adaptation.

2.3 Codification of European Values in Digital Policy Framework

European Values, including data protection, personal privacy, cybersecurity, digital inclusion, environmental sustainability, and fundamental rights protection, have been systematically embedded into digital policy instruments (GDPR, ePrivacy Directive, Data Act, AI Act, Digital Services Act). This represents a deliberate strategic choice to differentiate European digital

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

governance from alternative models, creating a unified ethical and governance framework that simplifies decision-making for companies operating across Member States.

This values-based framework builds genuine trust with European citizens and businesses, encouraging uptake of digital services and reducing friction in data sharing arrangements. It also establishes a global normative position: when other countries adopt privacy and cybersecurity standards, they increasingly adopt European models, effectively expanding European influence. Digital inclusion provisions ensure that continuum technologies benefit entire populations, not just early adopters or wealthy regions. By transforming what could be regulatory burden into a market differentiator and governance legitimacy, companies and public administrations operating within this framework build trust with stakeholders and reduce the fragmentation that would otherwise result from inconsistent values frameworks.

2.4 Strong Data Sovereignty Framework and Infrastructure

Europe has established the world's most stringent data protection regime (GDPR) and is implementing sophisticated data sovereignty mechanisms through initiatives like Gaia-X. These create practical assurances that data generated and processed in Europe can remain under European control, subject to European law and European enforcement mechanisms. The existence of secure, Europe-based data centres certified under emerging standards (particularly Gaia-X "Label 3" certification, which requires physical server location in Europe and compliance with European values) provides the infrastructure necessary to implement data sovereignty commitments.

This framework is essential for the computing continuum because continuum architectures necessarily involve data flowing across multiple processing nodes, from edge devices to cloud centres. Without credible data sovereignty mechanisms, this distributed architecture creates data control vulnerabilities. Gaia-X and similar initiatives address this by establishing federated governance models where data remains under known jurisdictional control. Cross-border data flow mechanisms (such as those being developed with Japan and other partners) establish protected pathways for data transfer while maintaining sovereignty principles. Given that data sovereignty addresses a genuine concern among customers, namely the fear that non-European actors will capture their data, it is not merely a matter of regulatory compliance but rather a genuine market demand. Companies in regulated sectors (finance, healthcare, government) increasingly require data sovereignty as a condition of technology adoption, creating a defensible market niche for European infrastructure and governance mechanisms meeting these requirements.

2.5 Digital Markets Act Creating Fair Competition and Ecosystem Opportunity

The Digital Markets Act (DMA) represents a strategic regulatory intervention designed to address the market concentration achieved by large non-European technology platforms (referred to as "gatekeepers": Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft). The DMA prevents these actors from leveraging their dominant positions to unfairly disadvantage competitors, requires data access and interoperability for competing services, and enables smaller actors to compete more effectively. For the computing continuum, the DMA prevents gatekeepers from using cloud or data centre dominance to foreclose competition in edge or IoT services and requires interoperability, preventing lock-in that would otherwise trap European companies in non-European technology stacks.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

By creating a level playing field where performance and innovation capacity matter more than inherited advantages (first-mover scale, network effects, data lock-in), the DMA shifts competitive advantage toward European entrants who bring technical sophistication, regulatory compliance and values alignment. It creates space for European cloud service providers and edge-computing innovators to compete on merit rather than being disadvantaged by anti-competitive practices, enabling SMEs and startups to build viable business models without first-mover capture by dominant platforms. This effectively handicaps non-European competitors while empowering European ecosystem participants.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

3 WEAKNESSES

3.1 Absence of a Unified EU Capital Markets Union

Despite decades of discussion, the EU lacks a true capital markets union, a single, integrated financial market for equity and debt capital across Member States. This fragmentation creates a critical disadvantage for financing large-scale technology projects. European companies pursuing computing continuum technologies face fragmented access to venture capital, growth financing and project financing. A promising European computing company may secure seed funding in one Member State but struggle to find growth-stage capital without relocating to US markets.

In contrast, the US venture capital and private equity markets operate as a single, deep, liquid market where capital flows to the best opportunities regardless of geography. China's state-directed capital allocation mechanisms similarly ensure large-scale funding for strategic technology initiatives. The EU's fragmented approach means that even when European companies have superior technology or market positioning, they may lack adequate financing to scale production, build manufacturing capacity or fund market entry in competitive sectors. While regulatory excellence matters, execution requires capital; computing continuum infrastructure such as data centres, edge facilities and network upgrades, requires multi-billion-euro investments that cannot be adequately financed through fragmented national capital markets.

3.2 Insufficient Regulatory Compliance Monitoring and Enforcement

Europe has created an extensive regulatory framework for digital markets but lacks systematic, EU-level enforcement mechanisms to verify compliance and penalise violations. Where regulations exist but enforcement is weak, the rules effectively fail to constrain behaviour, creating a situation where European companies face high compliance costs while non-European competitors operating in European markets may operate with minimal actual compliance burden. Fragmented national enforcement creates additional friction: a company compliant with regulations in one Member State may face compliance challenges in another.

This is particularly problematic for regulations like the GDPR, Data Act, and DMA, where enforcement should be consistent but in practice varies significantly by Member State. Weak enforcement also means that gatekeepers continue anti-competitive practices that regulations theoretically prohibit, because the actual penalty risk is low. Without robust, consistent enforcement, European companies gain no protection from regulatory compliance, and the burden of compliance falls disproportionately on those attempting good-faith compliance while competitors operating with minimal actual enforcement burden maintain competitive advantages.

3.3 Fragmented and Excessive Regulation Creating Market Fragmentation

Although the EU has created common regulatory instruments (AI Act, Data Act, DMA, DSA, CRA, etc.), implementation across Member States remains inconsistent. National regulators interpret rules differently, transposition into national law creates variations, and enforcement priorities differ. This creates a patchwork regulatory environment where a solution compliant in one Member State may face regulatory challenges in another. Additionally, some regulations

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

overlap or create contradictory requirements, forcing businesses to navigate conflicting compliance obligations.

For computing continuum deployment specifically, this fragmentation is particularly damaging. A federated cloud or edge infrastructure operating across Member States must navigate multiple regulatory regimes simultaneously. Small and medium enterprises (SMEs) lack dedicated compliance teams and cannot absorb the cost of managing multiple regulatory frameworks, pushing them toward either operating in a single Member State and losing scale economies, or relocating to jurisdictions with simpler regulatory environments. Excessive regulation, rules that impose compliance burdens disproportionate to the actual risk or duplicate other regulations, further exacerbates this problem by hindering the consolidation of European markets that is essential to the strategic vision of a "Digital Single Market". When regulations are fragmented or excessive, SMEs particularly cannot scale beyond their home market, reducing the pool of competitive European competitors and fragmenting computing continuum infrastructure itself.

3.4 Administrative and Bureaucratic Burden in Compliance and Funding Access

Compliance with digital regulations in Europe is administratively demanding. Regulations like the Cybersecurity Act and Cyber Resilience Act require formal assessments, periodic audits, vulnerability testing, documentation and reporting. For a startup or SME, these requirements entail a significant administrative burden: hiring compliance officers, implementing monitoring systems, maintaining documentation, etc. The burden is not merely cost; it is distraction from core innovation activities.

Additionally, access to public funding for innovation (e.g., Horizon Europe grants, national innovation programmes) involves lengthy application processes, complex evaluation criteria, extensive documentation requirements and extended decision timelines. An innovator pursuing urgent market windows cannot afford to wait 12-18 months for a funding decision. The bureaucratic burden of funding access effectively locks out nimble, fast-moving innovators in favour of larger organisations with dedicated grant administration teams. Implementation of regulations also varies across Member States, requiring companies to understand and comply with different national procedures, timelines and interpretation practices. This creates additional compliance complexity for any actor operating cross-border. Since administrative and bureaucratic burden imposes costs that scale poorly for small organisations, while large, well-resourced companies can absorb compliance and funding-access complexity, it creates a hidden tax on European innovation that particularly harms the ecosystem's capacity to generate new entrants and disruptive competitors.

3.5 Cyber Resilience Act Creating Unintended Barriers to Open Source

The Cyber Resilience Act (CRA), designed to improve cybersecurity of products and services, imposes requirements for vulnerability testing, audits, continuous support and security patching. These are reasonable requirements for commercial products. However, the CRA's application to open-source software, where development is often volunteer-driven, maintenance resources are limited, and commercial support models are nascent, creates unintended barriers that threaten the foundation of European digital infrastructure.

Open-source developers and maintainers now face formal compliance obligations they cannot reasonably meet without significant new resources. This creates two concerning outcomes: some open-source projects reduce activity or cease maintenance rather than incur compliance

burden, directly harming the availability of critical infrastructure software; and only well-funded, commercially-backed open-source projects (like those backed by Red Hat, Canonical, or comparable companies) can achieve compliance, effectively commercialising open source and reducing community-driven innovation. This is particularly damaging for the computing continuum, which depends heavily on open-source software for edge computing, IoT platforms, containerisation, data processing and networking. Rather than strengthening cybersecurity, the regulation risks reducing the availability and diversity of security-critical software by creating regulatory barriers to precisely the category of software that underpins European digital infrastructure, despite treating open source as equivalent to commercial products despite their fundamentally different development and support models.

3.6 User Concerns About Lock-in, Data Control and Security

Despite strict European data protection regulations, users, both individuals and organisations, harbour legitimate concerns about the adoption of cloud and continuum technologies. Concerns include: lock-in effects (difficulty switching cloud providers or extracting data); GDPR compliance burden (both for service providers and data subjects); cybersecurity risks from interconnected edge-cloud systems; and uncertainty about US cloud providers' obligations under the US Cloud Act (which requires US companies to disclose data to US government on request).

These concerns are not unfounded; they reflect real risks. They create friction in adoption of computing continuum technologies because organisations (particularly in regulated sectors) are uncertain whether adopting cloud or edge solutions will compromise data control or regulatory compliance. This hesitation slows market adoption and creates openings for non-European competitors to claim data sovereignty advantages. Until these concerns are addressed through concrete mechanisms such as workable data portability, transparent audit rights, practical lock-out prevention and verifiable data isolation, adoption will remain constrained, reflecting gaps between the regulatory promises of data protection and the lived experience of organisations attempting to operate within European regulatory frameworks while using cloud and continuum technologies.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

4 OPPORTUNITIES

4.1 Reforming EU Regulation and Competition Stance for a Unified Digital Single Market

A strategic opportunity exists to accelerate completion of the Digital Single Market by harmonising telecommunications regulations across Member States and promoting consolidation and cross-border operations in digital infrastructure sectors. The current patchwork of national telecommunications regulations (frequency allocations, infrastructure requirements, operational permits) fragments what could be a unified market. Removing these barriers would enable pan-European telecommunications and cloud infrastructure companies to operate on equal terms across Member States, facilitating consolidation by combining fragmented national operators into larger, more efficient entities capable of competing with global competitors.

This would accelerate infrastructure deployment (5G, 6G, fibre, edge computing facilities) by allowing operators to make investments based on European-scale economics rather than national silos. Specifically, harmonizing spectrum allocation, infrastructure sharing requirements, and cross-border interconnection standards would unlock billions in efficiency gains and accelerate computing continuum deployment. Regulatory harmonisation for a unified market converts regulatory fragmentation into market unity, which is particularly important for physical infrastructure (telecommunications networks, data centre facilities) where economies of scale are critical, since European-scale unified markets have historically outcompeted fragmented national markets.

4.2 Expanding the EU Chips Act to Accelerate European Semiconductor Capabilities

The EU Chips Act is a strategic industrial policy instrument aimed at increasing European semiconductor manufacturing capacity and reducing dependence on external suppliers. However, current funding levels and implementation timelines are insufficient to achieve the Act's strategic objectives. An opportunity exists to significantly expand the Act in terms of funding committed, scope of support and pace of implementation, including increased direct funding for new fabs (manufacturing facilities) in strategically important segments; accelerated public-private partnership models that share risk while enabling rapid deployment; and expanded support for chip design capabilities (particularly in advanced process nodes and specialised chips for edge computing and AI).

Given the geopolitical importance of semiconductors and the multi-year timescales required to build manufacturing capacity, ambitious public investment is strategically justified and necessary. Semiconductors are foundational to the computing continuum and to European technological sovereignty. Unlike many technology domains where Europe can innovate incrementally, semiconductor manufacturing requires multi-year, multi-billion euro commitments that cannot be made by individual companies or Member States and thus require EU-level strategic commitment and financing.

4.3 Implementing a Long-Term EU Quantum Computing Strategy

Quantum computing represents a frontier technology domain where Europe has research strength but lacks coordinated, large-scale investment strategy. An opportunity exists to

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

establish a long-term, well-funded, coordinated quantum computing programme spanning research, technology development and industrial application, including harmonised funding architecture across Member States (avoiding duplication), coordinated research roadmaps, development of quantum-classical hybrid architectures, and pathways to quantum-secure cryptography.

Such a programme should be explicitly positioned as strategic autonomy investment: quantum computing capabilities will be essential for cryptography, optimisation and AI applications in the future computing continuum. Early leadership in quantum-continuum integration could give Europe significant competitive advantage. It is important to note that this programme should have a time horizon of between 20 and 30 years and explicit tolerance for long-term, high-risk research, areas in which public research funding is most appropriate. This allows Europe to invest deliberately in a frontier technology domain with centuries-long strategic importance. Unlike incremental improvements in existing technologies where Europe lags, quantum computing is still in foundational phases where current research choices can shape the entire trajectory, enabling coordinated European strategy to create unique advantage.

4.4 Dismantling Administrative and Regulatory Obstacles Through Regulatory Streamlining and Unified Authority Architecture

A strategic opportunity exists to fundamentally simplify Europe's regulatory architecture by consolidating overlapping regulations, creating a unified digital regulatory authority, and establishing clear, streamlined compliance pathways. This should include consolidation of overlapping regulations into coherent frameworks rather than layered regulation; creation of a single European Digital Authority with clear primary responsibility for digital markets, competition and cybersecurity; simplification of Horizon Europe and other public funding mechanisms to reduce application and compliance burden; and establishment of explicit SME-tailored compliance pathways with reduced burden for companies below certain thresholds.

Additionally, this opportunity includes lowering administrative burden for accessing public funding by streamlining grant application processes, accelerating decision timelines and reducing documentary requirements. Government programmes should be redesigned to support rapid deployment timelines consistent with technology market cycles (12-18 months for decision cycles, not 24-36 months). This converts a major weakness (administrative burden) into a competitive advantage, since Europe's underlying regulatory vision (values-based, citizen-centred, competition-enabling) is sound; the implementation is unnecessarily burdensome. Streamlined implementation would maintain regulatory intent while dramatically reducing operational friction, particularly for SMEs, and is low-risk because it does not require regulatory changes, only administrative redesign.

4.5 Removing Cross-Border Regulatory Barriers to Unified Digital Operations

An opportunity exists to establish truly reciprocal recognition of regulatory compliance across Member States, where certification or compliance achieved in one Member State is automatically accepted in all others. This should include unified recognition of data protection compliance (organisations certified as GDPR-compliant in one Member State do not require recertification in others), unified recognition of cybersecurity certifications, unified recognition of AI Act compliance for high-risk systems, and unified spectrum and telecommunications licensing for cross-border infrastructure.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Additionally, establishing common frameworks for cross-border data flows, subject to data protection principles, would enable federated cloud and edge infrastructure to operate seamlessly across Member States. This directly enables the fundamental architecture of the computing continuum: distributed and federated systems that operate beyond national borders. Without reciprocal recognition, federated infrastructure must navigate 27 separate regulatory regimes, making it economically unviable. Reciprocal recognition converts fragmentation into unity while requiring only legal alignment (ensuring that all Member States' data protection implementations are genuinely equivalent) before establishing mechanisms that eliminate massive operational friction.

4.6 Scaling Digital Sovereignty Through IPCEI and Similar Large-Scale Strategic Initiatives

The Important Projects of Common European Interest (IPCEI) mechanism has proven effective at coordinating large-scale, multi-country, public-private initiatives in semiconductors (IPCEI-Semiconductors, IPCEI-Microelectronics) and cloud infrastructure (IPCEI-CIS). An opportunity exists to expand and deepen this model for computing continuum technologies, including additional IPCEIs explicitly targeting edge computing infrastructure, AI-specific cloud services, quantum computing, and secure communications systems; longer-term funding commitments (10-15 year timescales) that match technology development cycles; explicit mechanisms for technology transfer and capability building across participating companies; and mechanisms to ensure that IPCEI-developed technologies transition into sustainable commercial services.

IPCEIs are effective because they explicitly coordinate public and private investment, reduce duplication, align incentives, and create scale economies that individual Member States cannot achieve alone. Scaling digital sovereignty through IPCEIs leverages a proven institutional mechanism that has demonstrated success in other domains. The IPCEI model aligns public resources, private execution capacity and cross-border coordination, precisely the combination needed for large-scale continuum deployment, so expanding this model compounds its effectiveness.

4.7 Implementing EUCS+ Certification to Create Trusted, Competitive Cloud Infrastructure Market

The European Cybersecurity Certification Scheme for Cloud Services (EUCS+) is a EU-developed standard for cloud service security. An opportunity exists to systematically implement EUCS+ as the de facto standard for all cloud and edge infrastructure in Europe, with explicit government procurement preference and support mechanisms, including government commitment to procure only EUCS+-certified services; funding support to help cloud providers (particularly European SMEs) achieve EUCS+ certification; integration of EUCS+ into regulatory compliance frameworks so that certification counts as evidence of meeting cybersecurity requirements; and marketing support to communicate EUCS+ as a trust signal in global markets.

EUCS+ is effective because it is technically robust, developed by European cybersecurity expertise, and creates a unified standard that enables competition among providers rather than lock-in to any single vendor. Unlike proprietary security standards, EUCS+ is open and vendor-agnostic. This converts certification (a potential regulatory burden) into a market differentiator, allowing EUCS+-certified providers to compete globally on the signal of high security and European regulatory alignment. For European providers, EUCS+ certification is a competitive advantage; for non-European providers, achieving certification requires investment in alignment with European standards, creating friction.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft / Confédération suisse / Confederazione Svizzera / Confederaziun svizra — Swiss Confederation — Federal Department of Economic Affairs, Education and Research EAER — State Secretariat for Education, Research and Innovation SERI

5 THREATS

5.1 Innovation Constraints from Overly Strict AI and Emerging Technology Regulation

A significant threat exists that excessively strict regulatory requirements for AI and emerging technologies could slow European innovation below the pace required to compete globally. While the AI Act is generally well-designed, specific provisions such as stringent requirements for high-risk AI systems, mandatory impact assessments, and proof-of-compliance burdens, could create such high barriers to entry that only well-resourced organisations can develop AI solutions. If regulatory requirements become stricter than those in other major markets, European AI research and commercial AI development could progressively migrate to less regulated jurisdictions.

This is particularly concerning for AI applications within the computing continuum (edge AI, distributed machine learning, autonomous decision systems), where rapid iteration and deployment are competitively important. Additionally, if regulatory compliance timelines lag technology development cycles, regulations become obsolete before they are fully implemented, creating frustration and encouraging non-compliance. Since innovation is competitive and Europe regulates more strictly than competitors, European innovators face competitive disadvantage, particularly if regulatory burden increases for European companies while non-European competitors operate in less regulated environments. This could create a "brain drain" of AI talent and AI startups from Europe to less regulated jurisdictions.

5.2 Privacy and Security Concerns Limiting Trust and Adoption

Despite Europe's strong data protection frameworks, practical concerns about privacy and security in cloud and continuum environments remain. Concerns include the difficulty of verifying that cloud providers truly isolate and protect data, uncertainty about insider threats and state-level access requests, lack of transparency about data processing, and complexity of understanding who actually controls data in federated systems. These concerns are not irrational; they reflect real risks that, if not adequately addressed through transparent, verifiable mechanisms, will constrain adoption of cloud and continuum technologies, particularly in regulated sectors (finance, healthcare, government).

This is a threat because it directly prevents market growth and creates openings for competitors claiming stronger security or data control. Europe has strong regulatory frameworks but lacks practical, verifiable mechanisms for users to confirm that their data is actually protected as promised. Until mechanisms like trusted execution environments, verifiable encryption, transparent audit trails and enforceable data isolation become standard features of cloud and continuum services, adoption will remain limited, reflecting a genuine capability gap that must be addressed to unlock market potential.

5.3 Energy Costs and Dependence on External Energy Suppliers

Computing continuum technologies are energy-intensive. Data centres, edge computing facilities, and large-scale IoT deployments all require substantial electrical power. If Europe cannot control energy costs and sourcing, continuum deployment becomes uneconomical and creates strategic vulnerability. European energy costs are currently higher than in US and Asia,

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

partly due to energy source diversity (moving away from fossil fuels) and reliance on imported energy.

A threat exists that if Europe does not develop sufficient renewable energy capacity, maintain reasonable energy costs and diversify energy sourcing, computing continuum infrastructure will become economically uncompetitive globally. Additionally, energy dependence creates vulnerability: if external energy suppliers restrict supply for geopolitical reasons, computing continuum operations could be disrupted. Energy costs and dependence directly impact the economics of deploying computing continuum infrastructure. Unlike technology or regulation, which can be improved through policy, energy costs are partly determined by global commodity markets and partly by geography. Europe must proactively manage this threat through renewable energy investment, energy efficiency standards for data centres, and strategic energy sourcing.

5.4 Lagging Digital Transformation Across Traditional Industries

Europe possesses world-leading traditional industries (automotive, manufacturing, energy, chemicals, pharmaceuticals). However, these industries are digitalising more slowly than required to maintain competitiveness. If these "old economy" sectors do not rapidly adopt cloud, edge, IoT and AI technologies, they risk erosion of competitive position to more digitally advanced competitors. This is particularly critical for Industry 4.0, smart manufacturing, predictive maintenance, supply chain optimisation and digital sustainability tracking, all areas in which computing continuum technologies are fundamental enablers.

If European traditional industry does not accelerate digital transformation, competitiveness in these sectors will erode, leading to job losses and reduced economic dynamism. This cascades into reduced demand for computing continuum infrastructure in Europe, weakening the business case for European cloud and edge investment. Lagging digital transformation creates a self-reinforcing negative cycle: without strong demand from traditional industries, computing continuum infrastructure investment remains limited; without robust infrastructure, digital transformation becomes difficult. Breaking this cycle requires coordinated action to accelerate traditional industry digital adoption, a task beyond any single company's capacity.

5.5 Failure to Achieve a True Single Market for Computing Continuum Infrastructure

Despite decades of European integration rhetoric, a genuine single market for telecommunications infrastructure, cloud services and computing continuum technologies does not yet exist. National regulations still fragment the market, spectrum is allocated nationally rather than continentally, and operators must navigate 27 separate regulatory regimes. This fragmentation prevents the scale economies necessary to compete with unified global competitors.

If Europe cannot consolidate toward a true single market with continent-wide spectrum allocation, reciprocal regulatory recognition, and unified infrastructure governance, computing continuum deployment will remain hobbled by fragmentation. European companies cannot scale to global competitiveness within fragmented national markets; they will continue to be smaller, less efficient and less profitable than consolidated global competitors. This is a fundamentally self-inflicted threat: unlike external competitive threats which require excellence to overcome, market fragmentation is a policy choice. If Europe cannot make the political choices necessary to consolidate markets, it is essentially accepting competitive disadvantage as a permanent condition.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

6 Synthesis

Factor 2, “Framework Conditions”, presents a paradoxical strategic situation. Europe possesses world-leading regulatory frameworks that explicitly embed European values (data protection, fair competition, sustainable development, fundamental rights) into digital policy. Instruments such as the AI Act, Data Act, Digital Markets Act, and data sovereignty initiatives (Gaia-X) represent sophisticated, forward-looking governance that is increasingly adopted as global reference standards.

However, these regulatory strengths coexist with significant implementation weaknesses: fragmentation across Member States, excessive and overlapping regulatory requirements, administrative burden that disproportionately harms SMEs, insufficient compliance enforcement, and lack of unified capital markets and infrastructure governance. The result is a situation where Europe has exceptionally strong regulatory intent but inconsistent, fragmented execution. Companies operating in European markets face high compliance costs but inconsistent application; small innovators face bureaucratic barriers that large, well-resourced competitors can absorb; and fragmented national markets prevent the consolidation and scale necessary to compete globally.

Opportunities exist to convert these weaknesses into strengths through strategic reforms: streamlining and consolidating regulations to reduce fragmentation and administrative burden; establishing unified digital governance authorities to ensure consistent implementation; completing the digital single market through harmonisation of telecommunications and infrastructure regulations; significantly expanding strategic investment in semiconductors, quantum computing and computing continuum infrastructure; and scaling successful coordination mechanisms like the IPCEI model. Threats, including overly strict innovation regulation, privacy concerns limiting adoption, energy costs, lagging digital transformation in traditional industries, and persistent market fragmentation, underscore the urgency of moving from regulatory aspirations to implementation excellence.

The central strategic question for Factor 2 is whether Europe can maintain its regulatory leadership and values-based differentiation while simultaneously streamlining implementation, reducing burden and creating the unified market and industrial scale necessary for global competitiveness. This requires political will to make difficult choices: accepting some regulatory harmonisation that creates uniformity rather than perfect Member State customisation; consolidating fragmented infrastructure governance; and making substantial public investments in strategic technologies where private markets alone cannot achieve necessary scale.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI