

TECH7 JOINT DECLARATION

Strengthening trust and resilience
in the digital economy



bitkom

DIGITALEUROPE 



JEITA



 TECHNATION^{CA}

techUK



EXECUTIVE SUMMARY

Digital technologies are now central to economic security, geopolitical influence, and long-term competitiveness. Artificial intelligence, advanced connectivity, cloud infrastructure and data-driven innovation are transforming how economies grow, how public services are delivered, and how societies function. In this context, the resilience, security and openness of the global digital ecosystem have become strategic imperatives for G7 economies.

Digital infrastructure, cross-border data flows, and emerging technologies underpin productivity, supply chains, healthcare systems, and national security capabilities. Because this ecosystem is inherently global and interconnected, no country can address its challenges alone. Strengthened cooperation among G7 members and trusted partners is essential to ensure that digital transformation continues to drive innovation and shared prosperity while maintaining high standards of security, privacy, and accountability.

The French Presidency of the G7 in 2026 offers a critical opportunity to deepen coordination on digital policy and reinforce collective leadership. Building on discussions held during the TECH7 Summit in Ottawa in October 2025, and on the momentum of Canada's G7 Presidency, this Joint Declaration reflects the technology sector's commitment to support governments in advancing secure, innovative, and reliable digital ecosystems.

TECH7 also welcomes the progress achieved under **Canada's G7 Presidency in 2025**. Key initiatives (including the G7 AI Adoption Roadmap, the GovAI Grand Challenge, the Kananaskis Common Vision for Quantum Technologies, and the reaffirmation of Data Free Flow with Trust) mark an important shift toward implementation, scale, and international coordination. Sustaining this momentum will be essential to ensuring that these commitments translate into concrete outcomes.

TECH7 brings together leading technology industry associations from G7 countries and the European Union, representing companies that design, build, and operate the infrastructure and services underpinning modern economies. Drawing on this operational expertise, TECH7 provides concrete policy recommendations to address shared challenges, including cybersecurity risks, barriers to AI deployment, fragmentation in data governance, and emerging risks linked to quantum and dual-use technologies.

This joint declaration sets out the technology sector's priorities for G7 cooperation in 2026. It focuses on practical, coordinated actions to **strengthen resilience, enhance competitiveness, support innovation, and maintain trust in digital systems**. In an increasingly complex geopolitical environment, ensuring that digital ecosystems remain secure, interoperable, and open will be essential to sustaining economic growth and technological leadership.

SECURE OUR FOUNDATIONS

1 International collaboration, trust, and resilience

Technological innovation relies on complex and interconnected global value chains, and no single country or region can deliver comprehensive technological capabilities in isolation. At the same time, recent geopolitical developments have highlighted the importance of security and resilience in digital ecosystems.

Strengthening the competitiveness and technological leadership of G7 economies requires both deeper collaboration among trusted partners and the ability to develop and sustain critical capabilities within interconnected G7 ecosystems. This includes fostering secure, resilient, and diversified supply chains.

Collaboration with trusted technology providers is central to achieving these objectives. Trust in digital ecosystems cannot be reduced to one single factor, and it should be assessed through a holistic and risk-based approach. This includes governance, risk management, transparency, compliance with applicable legal frameworks, protection of sensitive data, and the ability to ensure long-term security, reliability, and accountability.

TECH7 calls on G7 leaders to:

Promote resilient and diversified digital value chains

Facilitate the circulation of trusted critical technologies within G7 and partner ecosystems, while strengthening supply chain resilience against geopolitical and hybrid threats.

Support collaboration with trusted technology providers based on clear, objective and risk-based criteria

Such collaboration should be grounded in governance, transparency, security standards, technical standards and respect for applicable legal and regulatory frameworks. This approach preserves technological choice while enabling governments and industries to manage risks and safeguard critical interests.

Foster open and secure markets

Ensure fair competition and innovation, while preserving the ability of governments to support strategic sectors and address national security, resilience, and public policy objectives.

Maintain a stable, predictable and rules-based international trade environment

Foster including dialogue among partners, while promoting high-standard digital trade frameworks that reflect shared values and support inclusive economic growth.

2

Cybersecurity and resilience of critical infrastructure

Digital infrastructure is a foundation of economic resilience. Cyber threats are increasingly sophisticated and now target interconnected supply chains rather than individual organisations. As critical sectors such as energy, health, finance, and transport become more digitally dependent, resilience must extend across the entire ecosystem, from infrastructure and networks to devices and software.

Artificial intelligence is strengthening cybersecurity by improving real-time detection, prevention, and response capabilities, while the threat landscape continues to evolve. This reinforces the need for greater alignment of cybersecurity standards across the G7 to reduce fragmentation and improve collective resilience. Although the G7 Action Plan on Secure and Resilient Digital Infrastructure provides an important basis for cooperation, companies operating across jurisdictions still face fragmented requirements that increase complexity and reduce effectiveness. Strengthening resilience therefore requires closer alignment among trusted partners and deeper cooperation between governments and industry, including the operationalisation of “secure by design” through procurement, common frameworks, and support for smaller actors.

Recommendations

TECH7 calls on G7 leaders to:

Promote interoperable cybersecurity frameworks and shared global standards

- Develop common G7 principles for integrating security-by-design approaches into public procurement of digital infrastructure, leveraging existing international cybersecurity standards and national approaches. These principles should cover the full lifecycle of systems, including the identification, modernisation, or retirement of obsolete technologies, while maintaining a risk-based and outcome-focused approach.
- Promote interoperability across G7 cybersecurity frameworks by leveraging international standards and reducing regulatory fragmentation, including for critical sectors, such as energy, telecoms, transport, health, and public administration.

Strengthen G7 cyber resilience and supply chain security

- Launch a G7 Cyber Resilience Initiative combining structured, bidirectional threat intelligence sharing and coordinated incident response. This initiative should bring together national cybersecurity agencies and trusted industry partners, building on existing

platforms such as ENISA while extending coordination to the G7 level.

- Strengthen cooperation on digital supply chain security by improving information-sharing, aligning risk assessment methodologies, and leveraging certification frameworks to reduce duplication and enhance interoperability.

Reinforce trust, encryption, and cross-border security cooperation

- Reaffirm end-to-end encryption as a cornerstone of digital trust and the integrity of communications.
- Encourage enhanced international cooperation to combat cross-border fraud, including engagement with United Nations and other public-private partnership frameworks, and promote alignment of principles for cross-sector collaboration.
- Ensure cybersecurity and resilience frameworks remain compatible with secure and trusted cross-border data flows, recognising that continuity and redundancy depend on interoperable and secure infrastructure governed by shared principles of security, governance, and compliance.

3 Trusted cross-border data flows

Cross-border data flows are essential to the modern digital economy, enabling trade, AI development, and research collaboration. The Data Free Flow with Trust (DFFT) framework provides the appropriate architecture to govern these flows. Under Japan's Presidency, G7 ministers reaffirmed their commitment to DFFT, emphasising the importance of trust built through legal frameworks, privacy safeguards, and interoperable standards. Under Canadian G7 presidency, the G7 emphasised the key role of privacy-enhancing technologies (PETs) to operationalise DFFT. TECH7 strongly supports this direction and welcomes continued momentum.

However, significant fragmentation persists. Data localisation requirements, divergent privacy regimes, and inconsistent governance frameworks continue to hinder innovation and scale. These challenges are particularly acute in the context of fraud, which is inherently cross-border, cross-platform, and increasingly AI-enabled, creating systemic risks for digital economies and public trust. Embedding fraud prevention as a core use case within trusted data-sharing frameworks can help ensure that security and innovation advance together.

Strengthening trusted and interoperable data flows is therefore a core resilience priority, ensuring continuity for research, supply chains, and AI deployment across the G7 while reinforcing economic stability.

TECH7 calls on G7 leaders to:

Accelerate trusted and interoperable data governance

- Accelerate DFFT operationalisation by moving from principles to concrete interoperable standards, common frameworks for cross-border data access, and the deployment of technical solutions like Privacy Enhancing Technologies (PETs) that enable trusted data flows while protecting privacy and security. This should include structured exchange of best practices and industry-government collaboration to co-develop implementation tools.
- Support the development of cross-border data spaces, data trusts, and interoperable data protection frameworks including PETs, to enable secure and responsible data sharing across jurisdictions.
- Enable trusted cross-sector data sharing for fraud prevention by establishing interoperable frameworks for real-time exchange of fraud intelligence across financial services, technology, and telecommunications sectors, supported by clear legal gateways, harmonised standards, and reduced fragmentation from inconsistent regulations and data localisation requirements.

Advance open and rules-based digital trade

Advance the WTO Agreement on Electronic Commerce by encouraging broader participation in the WTO "Declaration on Interim Arrangements for the Agreement on Electronic Commerce" and supporting its early entry into force. Accelerate domestic implementation processes across all participating countries to ensure timely and effective application.

SHAPE THE TECHNOLOGIES

4 AI deployment in strategic sectors

The Hiroshima AI Process established a strong international governance framework. However, governance alone is not sufficient without large-scale deployment. There remains a significant gap between AI's potential and its actual adoption in strategic sectors, including manufacturing, energy, transport, agriculture, and public services. The barriers are well known: skills shortages, limited access to high-quality data, fragmented regulatory requirements, and constrained compute access for SMEs.

TECH7 welcomes the 2025 G7 AI Adoption Roadmap and the SME AI Adoption Blueprint as an important shift from principles to implementation. We call on G7 governments to implement these commitments with urgency, in close collaboration with industry.

AI adoption is accelerating, but sustained policy action is needed to ensure that benefits scale across sectors and economies. Governments also represent a major opportunity for AI deployment at scale, particularly in public services, healthcare, infrastructure management, and emergency response. Early adoption improves efficiency and also signals confidence to the wider economy.

A core requirement remains regulatory coherence. AI cannot scale under fragmented rules on data access, liability, transparency, and conformity assessment. G7 coordination on these issues is therefore a competitive necessity.

TECH7 calls on G7 leaders to:

Build on the Hiroshima AI Process (HAIP) as the primary multilateral framework for AI governance interoperability
Use the HAIP Guiding Principles and Code of Conduct as the common foundation for aligning G7 approaches to transparency, accountability, and bias mitigation. Promote wider awareness of the Hiroshima AI Process among governments, regulators, and stakeholders.

Accelerate AI deployment through coordinated roadmaps and enabling infrastructure

- Implement the G7 AI Adoption Roadmap with concrete timelines and sector-specific national roadmaps co-developed with industry in priority sectors such as manufacturing, energy, transport, agriculture, health, and public services. Align these roadmaps across the G7 to share best practices and enable interoperability pilots.
- Ensure these strategies explicitly address real-world AI deployment and the enabling foundations required to support it, including sensing technologies, edge processing, and real-time, reliable networks.
- Support investment in AI infrastructure that serves strategic sectors. This includes cloud and edge compute capacity, data centres, and Digital Public Infrastructure. Simplify permitting processes and ensure efficient access to energy and other resources. Reiterate the importance of cloud computing as an enabler of AI adoption and of Digital Public Goods and Infrastructure.

Enable trusted data access and open innovation ecosystems

- Develop common frameworks for ethical AI data access across G7 jurisdictions, with clear safeguards for data protection, non-discrimination, and intellectual property.
- Support open and collaborative AI ecosystems, including open-source AI. Adapt regulatory approaches to the specific characteristics of open innovation. Promote access for students, developers, researchers, and industry to experiment with and adopt AI technologies.

Scale AI adoption and reduce regulatory fragmentation

- Make AI economically accessible for SMEs through incentives, vouchers, shared compute access, and public procurement that creates demand for AI-ready solutions.
- Reduce regulatory fragmentation by improving compatibility of G7 governance frameworks. This should lower compliance costs and enable cross-border and cross-sector deployment. Leverage global industry-driven standards to improve interoperability and scalability.

5 Quantum technologies and opportunities

Context and industry perspective

Quantum computing, sensing, and communications are moving from research to commercial viability. The G7 Kananaskis Common Vision for Quantum Technologies correctly identifies both the economic opportunities in areas such as finance, climate modelling, logistics, and research, and the significant security implications of quantum capabilities. TECH7 strongly supports this vision and calls for a shift from strategy to implementation.

Quantum technologies represent a strategic opportunity for trusted partners to co-develop capabilities. Coordinated investment, shared technology roadmaps, and interoperable frameworks will be essential to scale quantum ecosystems while ensuring security and resilience in a competitive global environment.

A key priority is cryptographic security. Quantum computing will eventually render current public-key encryption obsolete, creating a “store now, decrypt later” risk for sensitive data. Governments and critical infrastructure operators must therefore accelerate post-quantum cryptography migration. Standards bodies around the world, including NIST and ETSI, are already advancing relevant frameworks, and industry stands ready to support implementation through coordinated and practical migration pathways.

At the same time, early developments in quantum algorithms, hardware, and hybrid systems are beginning to shape future industrial applications. Early coordination and investment will be essential for G7 economies to both adopt and help shape these technologies while ensuring long-term strategic resilience.

TECH7 calls on G7 leaders to:

Coordinate quantum security, standards, and post-quantum migration

- Coordinate G7 approaches to post-quantum cryptography migration, including risk-based timelines aligned implementation of NIST and ETSI standards and global cooperation around global standards convergence. Provide guidance, toolkits, and support mechanisms to help SMEs and critical infrastructure operators plan and execute the transition.
- Reinforce alignment of quantum technology standards including support for ongoing standardisation work on quantum technologies in ISO and IEC, across computing, sensing, and communications to ensure interoperability and avoid fragmentation.
- Seek coordinated approaches to quantum-related export controls among G7 and like-minded countries to ensure consistency and risk-based implementation.

Accelerate quantum technology development and industrial deployment

- Accelerate lab-to-market pathways for quantum technologies through expanded funding for research, testbeds, and pilot deployments. Strengthen public-private partnerships to bridge the gap between scientific breakthroughs and commercial applications.
- Strengthen industrial integration by facilitating access to quantum infrastructure and enabling cross-border pilot projects. This should support companies in adopting quantum technologies across strategic sectors and accelerate real-world use cases.

Build a collaborative quantum innovation and talent ecosystem

- Support collaborative quantum R&D across G7 countries and like-minded partners through joint funding of cross-border pilot projects involving industry and research institutions. Promote researcher mobility and the development of specialised quantum skills pipelines.
- Share research roadmaps and best practices to improve coordination, maximise efficiency, and strengthen interoperability across the quantum ecosystem.

E Reinforce security of supply chains and digital infrastructure

Digital technologies sit at the intersection of economic competitiveness and strategic security. Semiconductors, AI systems, cloud infrastructure, encryption, and connectivity technologies underpin both economic growth and civilian and defence capabilities. Their dual-use nature is accelerating while regulatory frameworks remain fragmented. G7 coordination is therefore essential.

Supply chains and export controls. Digital value chains depend on trusted access to critical technologies. However, existing export control regimes for software-defined systems, cloud services, AI models, and cryptographic technologies would benefit from greater cooperation. G7 alignment in the development and administration of export controls is a resilience priority. It should preserve security while enabling trusted ecosystems to share and update critical technologies, and avoid unnecessary trade barriers within allied markets.

Satellite and connectivity infrastructure. Satellite systems and space-based infrastructure are becoming essential for global connectivity and resilience. They complement terrestrial networks and support critical functions including communications, climate monitoring, and emergency response. Next-generation connectivity, including 5G, 6G, and terrestrial-satellite convergence, is increasingly strategic. As networks become software-defined and integrated with space systems, harmonised standards and coordinated spectrum management are essential to ensure interoperability, resilience, and secure operations. In addition to space-based infrastructure, resilient and trusted optical fibre and cable infrastructure are crucial, underpinning high-speed, secure communications that enable critical services, and emerging technologies.

TECH7 calls on G7 leaders to:

Coordinate export controls and trusted circulation of dual-use technologies

- Align the development and administration of dual-use export control frameworks and strengthen coordination with like-minded partners to ensure coherent, risk-based implementation. The objective is to prevent adversarial access to controlled technologies while enabling trusted providers to deploy updates and innovations rapidly within allied ecosystems.
- Develop coordinated policies for the circulation of critical technologies across trusted G7-aligned ecosystems. This should preserve security while avoiding fragmentation that would undermine both collective resilience and industrial competitiveness.
- Reinforce alignment of quantum export control regimes across the G7 and like-minded countries as the technology matures, ensuring coordinated updates and consistent implementation to support secure development and adoption.

Strengthen resilient space, satellite, and connectivity infrastructure

- Align G7 approaches to space and hybrid connectivity networks, including 5G NTN, 3GPP, 6G, and open RAN. Promote interoperable and affordable terminal solutions, and support investment in space-based backhaul as a resilience layer.
- Modernise space and connectivity regulation by ensuring frameworks are evidence-based, aligned with international standards, and internationally consistent. Reform outdated spectrum-sharing rules that constrain non-geostationary satellite systems, and ensure broadband policies remain technology neutral, recognising the role of satellite connectivity in bridging the digital divide.

Integrate commercial digital innovation into defence capabilities

Develop procurement frameworks that enable G7 defence establishments to integrate commercial technologies, including AI, secure cloud, advanced connectivity, and encryption. This should strengthen interoperability across allied capabilities and improve the speed of capability deployment.

**MAKE IT WORK
FOR EVERYONE**

7 Health

The convergence of digital technology and healthcare is transforming health systems. AI, interoperable health data, and digital infrastructure can improve diagnostics, accelerate research, personalise care, and strengthen resilience against shocks such as pandemics and climate events. However, adoption remains uneven, and only around 60 percent of countries currently have a national digital health strategy.

Significant value remains untapped in health data, with up to 97 percent still underused for clinical and system-level decision-making. Artificial intelligence can help unlock this potential by enabling the analysis of large and complex datasets, supporting better diagnosis, more efficient systems, and more personalised treatments. Realising these benefits requires trusted frameworks for data governance, interoperability, and responsible AI deployment across jurisdictions.

G7 Health Ministers have already committed to open globally relevant standards, including HL7 FHIR and the International Patient Summary. The priority now is implementation. Without interoperable frameworks, digital health solutions cannot scale across systems or borders.

Healthcare is also one of the most cyber-exposed critical sectors. In 2023, EU Member States reported 309 major cyber incidents affecting hospitals and clinics. The EU Healthcare Cybersecurity Action Plan provides a useful model for proactive and layered defence, and could inform greater alignment across the G7. Industry is a key partner in delivering these protections but requires clear and harmonised requirements to invest at scale.

At the same time, digital health is accelerating biomedical research, clinical trials, and the development of diagnostics and treatments. Strengthening secure and trusted data-sharing frameworks is essential to enable collaboration between healthcare systems, research institutions, and industry, and to translate innovation into patient outcomes.

² G7 Health Ministers' Declaration on Open Standards

Recommendations

TECH7 calls on G7 leaders to:

Establish interoperable health data and enable AI deployment in healthcare

Support the adoption of HL7 FHIR and the International Patient Summary across G7 health systems. Develop governance frameworks that enable secure, trustworthy, and privacy-preserving use of health data, including appropriate cross-border secondary use in line with national regulatory frameworks.

Create enabling conditions for AI adoption in healthcare across the full lifecycle, from development to deployment and market entry. This should include responsible procurement standards and the secure digitisation of legacy records and paper-based systems as a foundation for scalable AI use.

Strengthen healthcare cybersecurity and resilience

Promote cybersecurity practices in healthcare aligned with international standards and relevant regional frameworks. Encourage secure-by-design principles for medical devices and hospital IT systems.

Support the development of a G7 health cybersecurity early-warning system and strengthen rapid incident response capacity across health systems.

Expand equitable access to digital health solutions. Remove barriers to telemedicine, digital therapeutics, and mental health platforms. Ensure that digital health innovation is designed to improve equity, including access for underserved populations and improved health literacy.

8 Skills and future of work

Context and industry perspective

Digital and AI skills are spreading unevenly across the workforce, particularly in SMEs and regions with limited access to training. While the tech sector is creating new roles in AI and data, the main challenge is not initial training but continuous reskilling as technologies evolve. SMEs are especially exposed, as they often lack the capacity to manage AI-driven workforce transitions.

At the same time, AI is creating new opportunities for work and entrepreneurship by lowering entry barriers. Addressing these shifts will require stronger cooperation between governments, industry, education systems, and training providers across G7 countries. The G7 must act decisively to avoid falling behind global competitors and ensure its economies remain adaptive and future-ready.

Recommendations

TECH7 calls on G7 leaders to:

Build an AI-ready workforce through skills systems transformation

- Strengthen public-private partnerships between governments, industry, universities, and training providers to expand access to AI and digital skills, with a focus on SMEs and mid-career workers
- Co-design curricula and continuously upskill educators and trainers in AI-related fields
- Develop national AI and digital skills frameworks aligned with evolving labour market needs

Enable workforce transition and mobility

- Support continuous reskilling across all job categories, enabling low- and medium-skilled workers to transition into AI-augmented and higher-value roles
- Ensure cohesive integration of new and existing job categories, avoiding labour market fragmentation
- Promote broader workforce mobility and mutual recognition of skills across economies

Strengthen public sector AI capacity

- Develop structured partnerships with industry to build AI literacy and applied skills across the public sector workforce, including civil servants, frontline workers, and procurement officials
- Strengthen governments' ability to deploy, manage, and oversee AI effectively

Support SME adaptation and workforce transition

- Develop practical tools for SMEs to assess skills gaps, deploy AI solutions, and manage workforce transitions
- Promote shared training platforms, industry-led programmes, and access to advisory services

Ensure equitable access to AI opportunities

- Promote skills-based hiring and inclusive workforce pathways
- Strengthen data governance practices, including representative datasets and bias testing to mitigate discrimination risks in AI systems

9

Enabling SMEs in the Digital Economy

Entrepreneurs and small businesses are a key driver of G7 economies and economic resilience. However, the digital economy still creates structural barriers for new entrants, including complex cross-border compliance, fragmented tax and registration regimes, and frameworks often designed for large incumbents.

In a context of rising costs, supply chain disruption, and shifting demand, the ability to start, scale, and adapt digital businesses is a core determinant of competitiveness. G7 policy should support, rather than hinder, this dynamic by reducing fragmentation and regulatory complexity.

TECH7 calls on G7 leaders to:

Reduce barriers to digital business creation and scaling

- Commit to lowering the time and cost of registering and operating digital businesses across G7 markets.
- Develop a G7 Digital Business Passport enabling mutual recognition of compliance across jurisdictions to reduce cross-border friction.

Simplify cross-border digital trade for SMEs

- Harmonise key aspects of VAT, customs, and consumer protection rules to reduce compliance asymmetry between large companies and SMEs.
- Establish de minimis thresholds aligned with modern e-commerce realities.

Ensure proportionate digital and AI regulation

- Design digital platform and AI regulation with SMEs and entrepreneurs in mind.
- Require regulatory impact assessments that explicitly evaluate burdens on micro-enterprises and solo entrepreneurs.

Expand access to digital infrastructure and tools

- Improve access to high-speed connectivity, cloud services, and AI tools for entrepreneurs across all regions.
- Support targeted programmes for first-time and underrepresented founders.

Promote open and interoperable digital markets

- Avoid digital protectionism and unnecessary localisation requirements that fragment markets.
- Support interoperability between platforms and payment systems to enable cross-border market access for SMEs.


A UNIFIED CALL TO ACTION

The Paris Summit presents G7 leaders with a defining opportunity. The recommendations in this declaration represent an integrated agenda for digital resilience, innovation, and shared prosperity, grounded in the realities of our industry and designed to be implementable.

We call on G7 leaders gathered in Paris to:

- Move from declaration to implementation: translate the commitments of the Canadian presidency and previous summits into funded, time-bound action plans with accountability mechanisms;
- Reduce regulatory fragmentation: prioritise harmonisation of AI, data and cybersecurity, frameworks across the G7, and leverage global standards so that our industries can operate and scale across borders;
- Invest in digital resilience as a long-term strategic asset: treat cybersecurity, AI infrastructure, quantum migration, and digital skills as infrastructure investments, not discretionary spending;
- Deepen public-private partnership: create structured, sustained mechanisms for industry engagement in G7 digital policymaking, beyond consultation on specific documents.
- Place entrepreneurship at the centre of the digital resilience agenda: commit to concrete, measurable reductions in barriers to starting, running, and scaling digital businesses across G7 markets, and to open, predictable cross-border digital trade rules that work for businesses of all sizes.

The technology sector across G7 economies stands ready to partner with governments in delivering these outcomes. We will continue to engage through the 2026 TECH7 Summit and the G7 Digital Ministers' Meeting to track implementation and sustain this collaboration.



Contributors

Anitec-Assinform

AFNUM

Bitkom

DIGITALEUROPE

ITI

JEITA

Numeum

TECHNATION

techUK

Graphic design

Studio Facette 2026



bitkom



JEITA



techUK