Navigating the Headwinds

D9+ Member States and their business communities have an important role in helping Europe to realise shared ambitions for this Digital Decade that safeguard prosperity, fairness, and resilience.

Executive summary points:

1. Digital leadership, partnership with enterprise and likeminded international partners are important to safeguarding EU resilience and navigating economic and societal headwinds.
2. As frontrunners, the D9+ EU Member States ('D9+') must help Europe shape and realise ambitions on digital leadership by collectively safeguarding trust, investment, and innovation. We, as the leading business federations in the D9+ States (the 'B9+ group') have made constructive contributions to D9+ discussions and remain ready to support the D9+ forum further in its work.
3. The EU and its Member States must accelerate momentum on Europe's Digital Decade initiative and on national digital agendas.
4. Intensify work with likeminded partners to lower global barriers to digital trade and innovation. Safeguard an open strategic autonomy approach, enable international data flows, leverage the EU-US Trade and Technology Council (TTC) and engage enterprise.
5. The EU must work with, not against, further digital and data driven innovation in the regulation and governance of AI and Data.
6. Ensure Cybersecurity Certification Schemes safeguard trust and a smart technological sovereignty approach. Consider and agree political issues politically, not at a technical level. Further engage industry, identify, understand, and address potential impacts.

Introduction

European economies and societies are facing into challenging headwinds, including health, environmental, energy and inflationary pressures, and the ongoing military aggression against Ukraine. Digital leadership and partnership with enterprise and likeminded international partners are important to EU resilience and navigating these headwinds. We must ensure resilience by safeguarding trust, investment, and innovation. Throughout the COVID-19 pandemic, trusted digital and data driven innovation and international co-operation have proven critical to our economic and societal well-being and will be essential to the EU's future success and resilience.

As frontrunners, the D9+ Member States[1] must collectively help the EU shape and realise ambitions on digital leadership, by safeguarding trust investment and innovation. We, as the leading business federations in the D9+ Member States (the 'B9+ group')[2] remain ready to support these efforts and have made constructive contributions on topics such as artificial intelligence (AI), the Digital Decade, the twinned green and digital transitions and transatlantic co-operation on digital[3]. While progress is being made, a significant step-change from our current trajectory is required across Member States in partnership with their business communities[4].

The shape of Europe's digital future matters. We welcome and encourage the ongoing joint efforts by our national government Ministers, and as the D9+, to proactively promote and enable trusted

[1] D9+ is an informal group of digitally advanced EU countries, including Belgium, Czech Republic, Denmark, Estonia, Finland, Ireland, Luxembourg, the Netherlands, Poland, Portugal, Spain and Sweden.
[2] Please signatories to this communication.
[3] See the B9+ Joint statements to D9+ Ministerial Meetings (a) Luxembourg, October 27, 2021 here and (b) Prague, March 29, 2022 here.
[4] European Commission (2022) Digital Economy and Society Index (DESI).

digital and data driven innovations and openness both at home, across the EU and with likeminded partners, strengthening our collective economic recovery, resilience, and well-being. In this context we offer the following recommendations:

Accelerate momentum on Europe's Digital Decade initiative and on national digital agendas.

1) **Enable further sustainable digital opportunities by deepening commitments from Member States, coupled with an integrated EU framework**. EU digital frontrunners should intensify the pace and level of Europe's collective digital performance by working with the Commission to finalise national and EU trajectories on digital to 2030, further demonstrating their success, building trust in digital transformation and deepening collaboration in building a shared and inclusive agenda. The EU and Member States should ensure strong governance to monitor spending and momentum for promoting and realising Europe's digital ambitions by 2030.

Intensify work with likeminded partners to lower global barriers to digital trade and innovation.

2) **Safeguard an open strategic autonomy approach which maintains** openness, access, innovation, and choice.

3) **Enable international data flows and leverage the EU-US Trade and Technology Council (TTC) and engage enterprise, including SMES and start-ups**[5]. The EU should enhance transatlantic research, economic and cybersecurity cooperation by agreeing on common approaches to strategic challenges in trade and technology:
    a. **Enable international data flows** to enable further economic opportunity in Europe. Explore common approaches to data governance, data portability and interoperability. Build on the momentum of the recent EU-US political agreement and swiftly deliver a revised and resilient overarching framework for EU-US data exchange, addressing privacy issues as well as the needs of modern digitalised business. The EU should work with OECD partners to deliver further policy guidance on data governance.
    b. **Strengthen collaboration, research cooperation, and develop market-driven standards in cybersecurity and emerging technologies**, including AI, the Internet of Things and 6G in line with WTO/TBT principles. We should strive for interoperability in frameworks by clarifying common regulatory requirements for EU-US health data exchange and deepening co-operation in digital health innovation.
    c. **Support a green and digital transition**. Explore common actions that leverage digital and data innovation in enabling a green transition.
    d. **Develop capabilities and capacities in our semiconductor ecosystem based on identified points of weakness and market demand and build on existing strengths**. Strengthen RDI and encourage further private investment by leveraging the TTC, to improve research and supply chain resilience.
    e. **Deepen digital skills**. Promote multiple skills pathways which foster further opportunities and success in a digital decade. We encourage Member States to share best practices on approaches and methods.
    f. **Ensure harmonised implementation and application to the regulation of digital markets and online safety**. Support contestability and fairness while ensuring non-

[5] The B9+ welcome the D9+ expressed support for stakeholder involvement in discussions on possible areas for digital cooperation between the EU and the US, see Prague meeting summary here.

discrimination, proportionality, and predictability. Consider flexibility in addressing the different needs and purposes of distinct sectors.

g. **Align on criteria for what technologies require export controls** and promote multilateral solutions.
h. **Exchange best practices on implementation of FDI screening**. Address concerns over an expanded definition of national security and the potential use of economic criteria in investment screening.
i. **Promote further SME access to, and use of digital technologies** by incentivising further digital adoption and increasing skills. Promote the uptake of digital tools in custom procedures including documentation and controls, and reduce costs for companies, especially SMEs, whenever possible.
j. **Champion further digital collaboration, innovation, and trade with likeminded partners in the WTO**.

Work with, not against, further digital and data innovation in governance and regulation. Safeguard trust in further digital opportunities.

4) **Stand up for a proportionate, human-centred approach to the governance and regulation of AI development and adoption, based on evidence and risk**. **Reassess potential administrative and compliance burdens**, particularly for SMEs, or unwanted consequences in the proposed AI Act which could discourage investment in the development and deployment of AI systems and consequently hurt Europe's twin digital and green transitions and its competitiveness.
    a. **Focus on where most widespread and significant societal damage is likely to arise** particularly in proposals around the definition of AI systems, the allocation of responsibilities between different actors in the AI value chain, criteria for determining prohibited practices and the classification of high-risk systems.
    b. **Focus the proposed definition of AI,** concentrating on AI systems that display intelligent behaviour and take actions with some degree of autonomy. The Commission's proposed definition of "AI systems" is too broad and would include most contemporary software and applications that use pure statistical and knowledge-based approaches for conventional data analysis that have little impact on individuals.
    c. **Regulate high-risk AI applications in areas where a clear regulatory gap has been demonstrated**. The EU should refine the Commission's proposed classification rules for high-risk AI to ensure consistency with sectoral legislation in Annex II, as well as to limit Annex III categories to use cases posing significant risk to health, safety and fundamental rights.
    d. **Reassess and clarify responsibilities of different actors in the AI value chain to ensure compliance**. The proposed compliance framework should be proportionate with a risk-based approach.
    e. **Support and enable efficient co-operation between relevant regulators at the national and EU level**. The legislation should support regulators and avoid fragmentation in the internal market by using sandboxes schemes, with well-established criteria to ensure an effective access to businesses, particularly SMEs. It should also support controlled experimentation by our innovators and regulators to assess (yet unforeseeable) risks, locate potential legal barriers and inconsistencies and develop solutions. Regulators should be adequately resourced to enable the development, deployment, and success of sandboxes. Avoid potential bottlenecks to

sandboxes and other related provisions, due to a lack of regulatory competencies, resources or cooperation between relevant regulators.

5) **Foster and safeguard our data economy for jobs, better services, health, and our environment.**
    a. **Develop a sustainable and responsible data-sharing environment which prioritises trust and a voluntary framework**. This should be subject to fair incentives, which safeguards privacy, security, and commercially sensitive information avoiding mandatory business-to-government (B2G) requirements.
    b. **Support B2B sharing** and develop spaces that facilitate easy and fair data sharing while maintaining contractual freedom as a guiding principle.
    c. **Avoid mandatory technical specifications for data portability which risks global fragmentation, reduce customer choice and slow innovation**. The EU should enable researchers and innovators to lead Europe's path to a more connected future and ensure our approach to data breaks down digital borders and improves the conditions for data mobility.

6) **Ensure Cybersecurity Certification Schemes safeguard trust.** We share the EU ambition to increase cybersecurity and trust in digital technologies. We should develop our indigenous cybersecurity ecosystem, while preserving an open economy and avoiding over-regulation. We should enhance co-operation across the EU and with likeminded international partners on cybersecurity and resilience. The Cybersecurity Act and the cybersecurity certification schemes being developed under this Act can play an important and necessary part in achieving this ambition. However, we have concerns about sovereignty requirements that may be added to the proposed European cloud certification scheme. In going forward, we respectfully recommend the following principles:
    a. **Consider and agree political issues politically, not at a technical level**. It is understood that the current draft of the "European Cybersecurity Certification Scheme for Cloud Services" (EUCS) contains proposed technical requirements and genuine political issues, in particular EU data localization and immunity from foreign laws requirements. Such political issues should be discussed and decided at the political level before being included in a certification scheme. A certification scheme, however, is not an appropriate instrument to decide political questions[6].
    b. **Further engage industry, identify, understand, and address potential impacts**. An impact assessment is needed to get a clear picture of the market implications (such as possible hinderance of innovation and growth, competition issues and practical implications). The fact that the scheme may be of a voluntary nature, does not exclude the necessity for a political decision regarding the possible geopolitical implications nor exclude the necessity for an impact assessment of the implications for the EU internal market also keeping in mind that the European Commission can through delegated (or implementing) acts mandate such certification schemes.

[6] The European Court of Justice states with regard to delegation of powers (Case C 355/10) that **"provisions which, in order to be adopted, require political choices falling within the responsibilities of the European Union legislature cannot be delegated**".

c. **Safeguard a smart technological sovereignty approach**. We support a 'smart technological sovereignty'[7] approach that encourages capacities across the EU while remaining open to further international co-operation and trade with likeminded partners so Europe can access and safeguard the economic benefits of further digital transformation.

[7] BusinessEurope (2020) Smart technological sovereignty: how it could support EU competitiveness