

Our position

EU guidelines on public procurement of cloud services

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.7 trillion in 2022, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Executive summary

The informal Member State Cloud Cooperation Group (MSCCG) that was established under the European Alliance for Industrial Data, Edge and Cloud, is developing guidelines on public procurement of cloud computing services (Guidelines). Such Guidelines could, in principle, introduce much-needed clarity and coherence to the European cloud market, as an instrument to facilitate compliance, reflecting best practices in self-regulation and simplifying implementation of relevant EU regulations. In this context, the Guidelines could support wider adoption and boost trust in the use of new technologies.

Unfortunately, the work of this group has been characterised for a lack of transparency and industry engagement, raising concerns about the impact that these Guidelines would have on the adoption and boost of new technologies in the EU. To ensure the forthcoming Guidelines are practicably implementable, we encourage authorities to engage in an open dialogue with cloud providers before they are finalised and published. Concretely, the European Commission should submit the Guidelines to a wide public consultation, open not only to all types of cloud providers, but also to all EU and national administrations and public agencies that use cloud services, to gather the widest possible feedback.

Against this background, this paper introduces our recommendations on what we believe are best practices and necessary components of a forward-looking and future-proof public procurement framework that fosters the adoption of cloud computing by the public sector, including our views around privacy and security, sovereignty, sustainability and energy efficiency, requirements and skills among others.

Introduction

Public administrations across the EU rely increasingly on cloud computing to fulfil their missions. It offers speed, scalability, agility and cost-effectiveness, as well as privacy and security features which benefit public authorities. These solutions also allow for new ways of work, which were essential during the COVID-19 pandemic and remain highly relevant today, particularly to reach the 2030 Digital Decade goals. Cloud computing is also required as a baseline for artificial intelligence (AI) deployment and for potentially ground-breaking AI use cases.

In this context, the MSCCG is developing a set of Guidelines to provide much-needed clarity and coherence to the European cloud market, which will facilitate compliance, reflect best practices in self-regulation and simplify implementation of relevant EU regulations. While the Guidelines are expected to introduce these important improvements to the European cloud market, the MSCCG's work has remained strictly confidential and lacked opportunities for dialogue with industry. As such, the Guidelines will fail to benefit from industry's experience and best practices, many of which already deployed in projects with governments and local authorities across Europe.

Cloud companies can act as digital transformation partners and advisors to public sector entities and offer their in-depth expertise to ensure successful deployment of cloud solutions in the public sector. Our members have long-standing customer relationships with European, NATO and OECD governments, helping administrations to better connect with and serve citizens. They not only comply

with the EU's regulatory framework for data protection, privacy and processing, but have also put in place robust measures to increase the control of European customers – including European governments – over their data. These measures include sophisticated security safeguards such as encryption tools, industry-leading contractual commitments to customers regarding the treatment and protection of their data, and partnerships with European technology providers.

Recommendations

As the Guidelines are still in development, we would like to offer our views to the European Commission and Member States on what we believe are best practices and necessary components of a forward-looking and future-proof public procurement framework that fosters the adoption of cloud computing by the public sector.

Privacy and Security

In a period of heightened geopolitical tensions and cybersecurity threats, Member States should retain the flexibility to procure the technology solutions that best meet their needs and provide them with the appropriate controls over their data. EU governments and public agencies need to have a broad choice of cloud providers that are best-in-class in privacy and security and provide assurances such as the application of internationally recognised standards and voluntary certifications (eg the ISO 27000 series or EU national schemes such as C5), and adhere to European best practices such as the EU Cloud Code of Conduct and the CISPE Code of Conduct to support their compliance with existing European legislation.

Sovereignty

Security and resilience are the main benefits of the cloud, and many EU governments rely on non-EU cloud providers that provide the highest level of security and resilience to meet their needs. As the EU and Member States are looking towards increasing 'data/digital sovereignty' in critical sectors, we support an approach to sovereignty that emphasises technical control over data, flexibility of choice, and frameworks aimed at generating trust and facilitating data flows, as opposed to blanket requirements for data localisation and/or EU headquartering or ownership.

Requirements based on providers' nationality do not enhance the security of the service or its data; they restrict choice and innovation and prevent interoperable approaches with like-minded partners that would otherwise encourage the growth and resilience of Europe's digital economy. Such requirements create lags in the region's digital transformation, outweighing the short-term benefits achieved for some Member States. European governments would have less choice of more expensive cloud services, which would diminish their resilience and place them at a disadvantage *vis-a-vis* their international competitors, particularly with regard to the uptake of advanced tools such as AI.

Hybrid multi-cloud approach

A multi-cloud approach offers public administrations the flexibility to choose the optimal configuration for resilience. A flexible multi-cloud strategy provides a solid foundation for portability and interoperability, reflecting considerations under EU legislation (such as Data Act and Digital

Markets Act). This includes using different cloud service providers for various applications and incorporating a combination of private cloud, public cloud and on-premises solutions that best suit their workload and data sensitivity.

Sustainability and energy efficiency

The European Commission has recognised that cloud and edge computing are among the digital technologies that will contribute to achieving the sustainability goals of the European Green Deal. Cloud computing helps to decarbonise business organisations, drive sustainable transformation of value chains and enable real-time decision making to shape sustainable business practices, including emission reduction, to mitigate climate risks. Conversations around advancing common metrics for measuring the sustainability of data centres are essential aspects of the revision of Energy efficiency rules and as a contribution to the achievement of climate neutral data centres by 2030. Several of our members also participate in the European Green Digital Coalition. Public procurement Guidelines should reflect on the importance of energy-efficient data centres, which will be essential for the sustainable use of cloud and edge technologies.

Consistency of the framework

Any new Guidelines should take account of, build on and be well articulated with existing requirements such as those contained in the Network and Information Security Directive II (NIS II), Artificial Intelligence Act (AI Act), Data Act, Data Governance Act (DGA), Cyber Resilience Act (CRA) and potentially the European Cybersecurity Certification Scheme for Cloud Services (EUCS). Duplicative, overlapping and potentially deviating requirements would lead to legal uncertainty and confusion, which in turn will diminish trust, coherence and clarity.

Avoiding prescriptive requirements

As public authorities transition towards a Cloud First approach, prioritising cloud-based solutions over on-premise options, it is important that they are supported in developing procurement strategies that promote cloud innovation, follow risk-based approaches and deliver the highest levels of security. The European Commission and Member States should support competence building so that procurers can design their tenders based on commercial cloud industry standards and best practices (including industry-recognised accreditations and certifications). This can avoid placing unnecessary restrictions on the services they can use and ensure access to innovative and cost-effective cloud solutions, without compromising on security controls, privacy or auditing capabilities. Policymakers should conduct market assessments before the development of framework requirements and/or a tender, which would reflect appropriate decision-making. Consultations with technology providers will ensure that clear information on the services available, resulting in future technology being built around best practices, compliance and security.

Diversity of the market

Different cloud users have different needs and business models, which provides for a vibrant and innovative ecosystem. They should be able to benefit from the best-in-class services offered by different providers as the most suitable for their needs. The Guidelines should acknowledge this complex and varied user landscape by recognising that they do not represent an exhaustive list of regulations and self-regulatory tools that all cloud providers need to comply with in the same way.

Cloud users need to remain in charge of selecting the cloud providers that best meet their technological and regulatory needs, and this requires a recognition of the very diverse landscape.

Skills

For the public sector to take full advantage of the opportunities presented by the adoption of technology and the digital transformation, it is critical to equip its employees with the right skills. These should be at the centre of European efforts on digital transformation. Alongside procuring technology, Member States should prioritise skilling initiatives for their governments' workforce in order to create an enabling environment and attract and retain talent that drives successful digital transformation. Partnerships with the private sector in this area can be particularly useful, given the vast expertise and comprehensive training and skilling programs that many cloud providers have already put in place.

Building trust and confidence

With increasing demands by the public sector for enhanced data privacy and security safeguards in the cloud, the European Commission can establish a foundation of trust between EU governments and industry stakeholders by fostering open communication channels through a structured dialogue.

Conclusion

In light of the vital role that cloud-computing plays for public administrations across the EU, policymakers need to develop a framework for public procurement that enables innovation, flexibility and customer choice, and that abides by the WTO Government Procurement Agreement. This will benefit European governments and citizens alike, and it will help deliver the EU's Digital Decade targets without creating artificial market access barriers for the adoption of cloud computing.