Joint Industry Statement on the Draft
European Cybersecurity Certification Scheme for Cloud Services (EUCS)

1 December 2022

We, the undersigned global business associations, are committed to helping contribute to a competitive, resilient and technologically-advanced cloud computing ecosystem in Europe. For this reason, we call upon EU Member State governments, the European Commission, the European Parliament, and ENISA to address our concerns about the future European Cybersecurity Certification Scheme for Cloud Services (EUCS). The signatories urge the EU to refrain from adopting requirements of a political – rather than technical – nature, which would exclude legitimate cloud suppliers and would not enhance effective cybersecurity controls.

The 13 associations represent both cloud customers and cloud vendors operating across the European Digital Single Market that have already made substantial investment contributions across numerous industries to build a thriving digital ecosystem in Europe. Our members include numerous organisations of all sizes that rely on first-class digital technologies to deliver their services and products in the EU and beyond. Our members seek to build a competitive, innovative and resilient digital economy while upholding shared values and interests of data privacy, effective cybersecurity protection, and supporting open markets.

We believe that an inclusive and non-discriminatory EUCS – supporting the use of the most innovative, and trusted cloud services from around the world – will help our members and their customers prosper at home and abroad, thus contributing to Europe's digital ambitions and strengthening its resilience. Regrettably, the draft EUCS includes several "immunity requirements"[1] that raise questions on compliance with the WTO's General Agreement on Trade in Services and the EU's Government Procurement Agreement commitments.[2]

---

[1] "Immunity requirements" known as immunity from non EU-laws, include among others certification eligibility restricted only to cloud providers globally headquartered in the EU, exclusion of vendors wholly or partially owned by an entity headquartered outside the EU, prohibition to store and process data outside the EU, and customer support capabilities restricted to employees located in the EU.

[2] The EU has taken on broad obligations to allow for the non-EU supply of computer and related services in both the government procurement market and the purely commercial market (the latter implicating restrictions in EUCS designed to apply to "critical infrastructure", that may be owned by private companies).

These EUCS requirements are seemingly designed to ensure that non-EU suppliers cannot access the EU market on an equal footing, thereby preventing European industries and governments from fully benefiting from the offerings of these global suppliers. If other countries were to pursue similar policies, European cloud providers could see their own opportunities in non-EU markets dwindle. Fragmentation of global cloud computing markets would hinder the long-term competitiveness of European firms as well. What is more, even European providers might find it hard, if not impossible, to meet the requirement on independence from non-EU laws.

As associations representing global industries that rely on cloud solutions, our members need access to the widest range of innovative cloud technologies that best suit their needs to be successful in a fast-growing global market. Unfortunately, as currently considered, the EUCS "immunity requirements" would considerably reduce cloud offerings in Europe, increase costs, result in cumbersome governance models that would not support customers' global needs, and likely delay adoption of the most up-to-date technologies. If, as the European Commission suggests, the EU wants "75% of Union enterprises" to take up "cloud computing services, big data, and artificial intelligence"[3] it should seek to expand – not decrease – the availability of cloud technologies in Europe.

As representatives of businesses that operate internationally, we believe that every market participant should have a fair chance to compete on merit, regardless of the location of their headquarters, the nationality of their shareholders or board members, or the business opportunities they may have pursued elsewhere. Yet, the suggested "immunity requirements" in the draft EUCS – which echo restrictive approaches member states have embraced in the past – would restrict competitive opportunities on this basis, and paradoxically undermine cybersecurity at the same time. For cloud service providers headquartered outside of the EU and their EU customers, this measure would require significant investments in time and resources to adapt their technical operations and legal structures; increasing costs, limiting flexibility, undermining resiliency, and delaying integration of latest technologies. Even then, they may not be able to achieve the highest level of certification – simply because of the location of their headquarters or the nationality of their investors – thereby undermining their ability to compete fairly for other economic opportunities.

At a time of unprecedented collaboration in the face of common global threats, a focus on exclusionary policies that targets Europe's most important international partners is particularly inopportune. We urge European governments to reject the inclusion of "immunity requirements" in the EUCS and ensure that any future certification, or similar broadly-spread common specification or standard, remains non-discriminatory and technically feasible.

- ACT | The App Association
- Coalition of Services Industries (CSI)
- Internet and Competitive Networks Association (INCOMPAS)
- Japan Association of New Economy (JANE)
- National Foreign Trade Council (NFTC)
- techUK
- United States Council for International Business (USCIB)

- American Chamber of Commerce to the European Union (AmCham EU)
- Computer & Communications Industry Association (CCIA Europe)
- Information Technology Industry Council (ITI)
- Latin American Internet Association (ALAI)
- Software & Information Industry Association (SIIA)
- U.S. Chamber of Commerce

---

[3] See Commission Decision establishing the 2030 Policy Programme "Path to the Digital Decade"