Joint industry statement on the need for a swift adoption of the EU Cybersecurity Certification Scheme for Cloud Services without sovereignty requirements

Our organisations represent both cloud customers and cloud vendors operating across the European Digital Single Market. We call on policymakers in EU Member State governments, EU institutions and the European Union Agency for Cybersecurity (ENISA) to **firmly reject the proposed sovereignty requirements in the EU Cloud Services Certification** (EUCS) with a view to **a swift adoption of a workable and non-discriminatory EUCS**. Such sovereignty restrictions are politically motivated and do not add value to cybersecurity of cloud services in the EU. For well over a year, many European and international associations[1][2], industry actors and Member States[3] have continued to publicly express their concerns with the lack of progress and the ongoing examination of restrictive sovereignty requirements in the EUCS. In addition, several Member States have **proposed alternative options to end the stalemate[4],** such as a European evaluation mechanism based on trustworthiness for non-EU cloud providers. Discussion on these proposals could offer a robust alternative that would meet the desired high level of cybersecurity requirements, while keeping the market open to all cloud providers.

We understand that a new draft of the EUCS was recently shared with Member States. According to accessible reports and information, the new EUCS draft from May 2023 maintains non-technical requirements – including absence of effective control from non-EU entities, independence from non-EU law and strict data localisation requirements – while the scope of application remains overly broad and unclear. In this context, we would like to reiterate the following concerns:

1. **Limited transparency and lack of stakeholder engagement**[5] – there continues to be a lack of transparency and detailed impact assessment, as well as very limited stakeholder engagement. Despite active requests from the involved governments and formal industry stakeholders.

2. **Inclusion of 'digital sovereignty' requirements** – involving corporate ownership requirements, immunity against non-EU law[6] and data localisation in the EUCS scheme would:

    a) Create significant barriers to entry for non-EU headquartered companies and EU companies with international/global operations and investments, which would limit competition in the cloud market, raise the cost of cloud services and limit the choice of trusted technology partners for European businesses.
    b) Endanger international cooperation on sharing threat intelligence, detecting cyber threats and vulnerabilities, and exploring joint solutions to tackle cyber resilience in the current geopolitical environment.
    c) prevent the great majority of non-European cloud providers from offering their services to those EU customers that would require a 'high' level of certification. This would limit considerably the market uptake of certification and delay the digitisation of EU services and processes beneficial for EU citizens and businesses.
    d) Push other jurisdictions to also introduce these requirements. Indeed, some countries like the US, whose current FedRAMP regime (Federal Risk and Authorization Management Program) focuses on the technicalities of cloud cybersecurity without imposing equivalent sovereignty measures, could be adapted to include ownership requirements and by doing so contribute to increased fragmentation in cybersecurity solutions among the

[1] See paper by the Association for Financial Markets in Europe AFME: https://www.afme.eu/Portals/0/DispatchFeaturedImages/230310_AFME%20Comments%20on%20EUCS_FINAL.pdf

[2] See paper by European Center of International Political Economy (ECIPE): https://ecipe.org/publications/resilience-cybersecurity-economic-trade-impacts-cloud-immunity/

[3] See the German-Dutch statement here: https://www.government.nl/documents/diplomatic-statements/2023/03/27/joint-declaration---government-consultations-netherlands---germany-27-march-2023. Other comments also available here: https://www.euractiv.com/section/cybersecurity/news/eu-countries-seek-way-out-of-impasse-on-sovereignty-requirements-for-cloud-services/.

[4] See Euractiv article here: https://www.euractiv.com/section/cybersecurity/news/eu-countries-seek-way-out-of-impasse-on-sovereignty-requirements-for-cloud-services/

[5] As stated also at the ENISA Certification website: https://certification.enisa.europa.eu/#

[6] Independence to non-EU Laws, which require: a/the CSP in question being globally headquartered in the EU and b/the entity in question who has no head office in an EU Member state, shall not directly or indirectly, individually or jointly, hold effective control of the CSP applying for the certificate

West.[7]

e) Limit European companies' business expansion opportunities to non-EU markets. In fact, the sovereignty requirements, and immunity to non-EU legislation, will also apply to the European companies, challenging their access to non-EU markets where they will be subject to third-country legislation.

3. **Conflicting Member States' views** –The prolonged informal stalemate among the public stakeholders, and the lack of agreement between Member States, may result in certain countries opting out from the scheme which would increase fragmentation, reduce trust and increase compliance costs for the industry.

4. **Legal confusion and uncertainty caused by the interplay with other EU legislation** – a swift adoption of a workable EUCS is necessary to ensure **alignment with existing and upcoming EU legislation**. For instance, Cybersecurity Act (CSA) foresees that the European Commission (Commission) should assess by 31 December 2023 the efficiency and use of a scheme and whether it should be made mandatory[8]. At this stage, it is unclear how the assessment will be conducted, if none of the announced certification schemes has been adopted. Secondly, various EU laws (eg the CRA), operate clearly with EUCS as a functional certification scheme; while others (eg DORA and NIS2) require further legal clarity to avoid regulatory compliance challenges for entities in scope of (both) regulation.

5. **Compliance with a World Trade Organisation (WTO) rules–** the European Commission should evaluate the consistency between the WTO and the proposed EUCS measures to ensure that the ownership and localisation requirements do not run afoul of the EU's WTO commitments (specifically under the General Agreement on Tariffs and Trade, the Agreement on Trade-Related Investment Measures, the General Agreement on Trade in Services and the Agreement on Government Procurement, among others).

The European Commission must swiftly adopt the EUCS by resolving the political deadlock and decide not to conflate legal and cybersecurity considerations in a technical instrument as we, and so many other stakeholders, have been publicly urging for since 2021[8]. Any EU cybersecurity certification **scheme should focus on technical measures to strengthen security and resiliency and, it should rely on and be aligned with consensus-based international standards that have proven to be efficient by way of broad industry adoption. There are options that enable a workable solution which does not include challenging requirements.** These should be explored in a separate political process detached from the speedy implementation of the cybersecurity scheme. **Members of the ECCG, ENISA and the Commission should proactively inform stakeholders on the status of the draft scheme in order to allow them to meaningfully contribute to the discussion before its submission.**

List of co-signatories:

- American Chamber of Commerce to the European Union (AmCham EU)
- ACT | The App Association
- BSA | The Software Alliance and the Global Data Alliance
- CCIA - Computer & Communications Industry Association
- Coalition of Services Industries (CSI)
- ITI - The Information Technology Industry Council
- Japan Association of New Economy - JANE
- Latin-American Internet Association - ALAI
- National Foreign Trade Council
- Software & Information Industry Association (SIIA)
- techUK
- U.S. Chamber of Commerce
- U.S. Council for International Business (USCIB)

[7] See paper by Information, Technology and Innovation Foundation (ITIF) here: https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/

[8] Some of these stakeholders include: EACH (https://eachccp.eu/wp-content/uploads/2022/08/EACH-Letter-Cybersecurity-Certification-Scheme-for-Cloud-Services-August-2022-2.pdf) and BDI (https://english.bdi.eu/media/publications/#/publication/news/european-cybersecurity-certification-scheme-for-cloud-services-eucs/)