AMCHAM

AMERICAN CHAMBER OF COMMERCE IN SWEDEN

The Home of American Business

Industry Letter Ahead of the TTE council on Dec 5th

As telecom and digital ministers from EU Member States meet on Dec 5th, European technological leadership and competitiveness top the agenda. In this context, we wish to express concerns regarding the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and its potential negative impacts on the state of cybersecurity, cloud adoption and technological development in Europe, particularly on generative AI development in critical sectors. We ask that this issue be discussed at the council meeting given the broad economic, technological, and trade implications.

The EUCS is a pan-EU scheme that can be made mandatory by EU regulations, local laws and procurement guidelines. We support the goal of EUCS to unify and harmonize best cloud security practices in Europe and we believe the continued delays in the adoption process are detrimental to EU's state of cybersecurity. However, **we are concerned about requirements in the current draft (leaked to media on November 22nd) that prohibit Cloud Service Providers (CSPs) which are not headquartered in Europe and fully owned by an EU entity to qualify for the highest level of EUCS certification.** In the current text, the highest level of certification is intended to apply broadly to data related to public order, public safety, public health or the performance of essential governmental functions.

This risks cutting off European businesses and governments from the most secure cloud services and cyber protections at a time when these institutions continue to be negatively impacted by malware, ransomware and DDOS attacks. Discriminating against CSPs based on country of origin would also introduce complexities and costs for European companies operating across jurisdictions, as they would no longer be able to scale efficiently. EU startups operating globally would face increased complexities and costs. The wide-ranging effects of this policy will be felt across the entire cybersecurity ecosystem, including on European companies such as subcontractors, involved in cloud service deliveries.

Additionally, customers using AI and Generative AI would face limitations on leveraging the benefits of global cloud infrastructure and access to diverse datasets, hindering the quality and diversity of models. For healthcare and life sciences, access to international datasets and scaling access to the latest medical tech are essential to accelerate the pace of innovation and improve lives.

While debated extensively over two years, the scheme has seen minimal changes despite industry pushback. Industry concerns are reflected in over 40 position papers and letters since 2022, left unanswered by the Commission and ENISA.

In the absence of an impact assessment by the Commission, attempts have been made by think tanks to model scenarios. One study warns Europe could lose €29-610 billion yearly, disproportionately affecting smaller states.

Banning non-EU providers is a political decision with broad economic and trade implications, one that should involve discussion between Member States. We know views among Member States differ significantly, and worry this tactic could enable protectionist policies without political debate.

Moreover, the current discriminatory approach risks favoring Member States with a more developed cloud industry while limiting access for other Member States to critical technologies and affecting future investments by non-EU cloud providers in Europe.

The Cybersecurity Act already gave a clear mandate to ENISA on EUCS and sufficient flexibility for Member States to adopt stricter national measures in certain conditions. EUCS will not override or in any way prevent Member States from adopting dedicated certification schemes for national security workloads. Also, Member States may impose additional or stricter cybersecurity requirements for the use of ICT products by essential or important entities, provided they are not covered by EUCS. This includes restrictions on services or suppliers that take account of non-technical factors.

Furthermore, the EU has adopted regulation for the protection of both personal and non-personal data, including protection from third-country law, under the GDPR and the Data Act. These regulations have been debated under normal EU legislative procedure with Member States input and stakeholder consultation.

Our letter comes ahead of the next and potentially final round of discussions between the Commission and Member States, to take place in the second week of December ’23, before the scheme reaches a voting procedure as an implementing act. We ask you to request a political discussion regarding the EUCS process and its unaddressed broad implications at the next telecommunications council. It is our belief that this important issue merits debate beyond the technical level and Member States should have an opportunity to discuss legal requirements at the political level and under the normal EU legislative process.

Finally, we strongly believe the solution to address data sovereignty concerns in the EU needs to be a technical and not a political one. For the sake of cybersecurity and technological advancement, technology providers should be allowed to innovate and compete on technical approaches.