EU Cybersecurity Certification Scheme: no more delays

The American Chamber of Commerce to the EU (AmCham EU) **calls on the European Commission, Member States and European Cybersecurity Certification Group (ECCG) experts to swiftly adopt the European Union Cybersecurity Certification Scheme for Cloud Services (EUCS) in the form presented by the European Union Agency for Cybersecurity in the draft of March 2024**. This draft strikes the right balance between ensuring freedom of choice for cloud users and implementing appropriate high-level technical and organisational safeguards to protect the data of European enterprises, public administrations and critical workloads.

The introduction of so-called 'sovereignty criteria' in a harmonised technical instrument like the EUCS would defeat its purpose of boosting the EU's cyber resilience, inserting discriminatory criteria that limits users' freedom of choice. Therefore, any adoption of the draft should remove the 'primacy of EU law' criteria to ensure that third-country cloud users can contract according to standard industry practice. The discussion of these criteria has already significantly delayed the EUCS, leaving European companies vulnerable in cyberspace.

The EUCS should allow companies in the EU to access the best-in-class cybersecurity solutions offered by trusted Cloud Service Providers (CSPs) – even if these providers are not headquartered in Europe. Thanks to considerable investments in cutting-edge technology and engineering talent, global CSPs are among the best-defended organisations in the world. This view is reflected in Mario Draghi's recent competitiveness report, which emphasises the need for a pragmatic EU approach to cloud services: 'It is too late for the EU to try and develop systematic challengers to the major US cloud providers: the investment needs involved are too large and would divert resources away from sectors and companies where the EU's innovative prospects are better... The EU must find a middle way between promoting its domestic cloud industry and ensuring access to the technologies it needs'.[1]

As noted by many European associations representing key strategic sectors – including critical infrastructure – an **EUCS containing criteria regarding the protection of European Data against unlawful access would limit cloud users' freedom of choice and jeopardise existing strategic partnerships with non-EU CSPs.**[2] These organisations have repeatedly stated that European CSPs do not offer the same technological capabilities as non-EU CSPs operating within the EU Single Market. Switching providers could potentially impact their operational resilience, cybersecurity level and competitiveness in international markets.

The Commission should therefore allow European companies leading in digital technologies, like artificial intelligence, to use cloud infrastructure from non-European providers. AmCham EU members are making substantial investments in the EU Single Market and developing solutions to provide European companies with safe, innovative and scalable cloud infrastructure. Sovereignty criteria, particularly ownership control clauses

[1] The future of European competitiveness, Report by Mario Draghi, Par A, A competitiveness strategy for Europe, Key barriers to innovation in Europe, p. 30.

[2] See examples: https://www.amchameu.eu/system/files/position_papers/spcr_joint_stament_eucs_20240617.pdf; https://globaldataalliance.org/news/gda-leads-call-to-adopt-eu-cyber-certification-scheme-eucs/; https://www.insuranceeurope.eu/mediaitem/ea37c654-f7f4-481c-9480-ac0eb9bf12ca/Joint%20Statement%20on%20EUCS.pdf; https://www.ebf.eu/wp-content/uploads/2023/11/Joint-Statement-on-EUCS.pdf; https://english.bdi.eu/publication/news/european-cybersecurity-certification-scheme-for-cloud-services-eucs.

and jurisdictional restrictions, would be difficult to operationalise, likely creating legal barriers and increasing costs – even in partnerships between European companies.

The Draghi report and President von der Leyen's Mission Letter to Commissioner-designate Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy, both underscore the crucial role of cybersecurity in supporting Europe's economic resilience, competitiveness and innovation capacity. The longer the EUCS's implementation is delayed, the longer Europe has to wait to strengthen its cybersecurity resilience. To avoid delays, **the ECCG and EU Member States should swiftly adopt the EUCS in its current form**. Looking ahead, the Commission should also establish **a leaner and faster approach to developing EU cybersecurity certification schemes**. These are essential steps for providing the harmonised cybersecurity standards and access to secure cloud innovation that European companies need to bolster the EU's digital economy.