Cybersecurity Certification Scheme for Cloud Services

The American Chamber of Commerce in the European Union (AmCham EU) welcomes the progress made on the Cybersecurity Certification Scheme for Cloud Services (EUCS). A robust EUCS framework can bolster trust in cloud services and foster innovation across the European Union. However, there must be further steps taken to ensure the scheme is effective, transparent, and that it aligns with international best practices.

Alignment with existing standards and open consultation

Several concerns have been raised by European stakeholders regarding the potential risk of unlawful data access, the need for clarity and consistency across the European market, as well as the importance of offering users clarity and transparency about the level of protection of their data. However, as detailed in our previous publication[1], obliging a Cloud Service Provider (CSP) to offer at least one option where the storing and processing of meta-data and cloud derived data does not give security or privacy benefits. It is already a best practice in the EU market to process and store CSC (Customer) data, for example in a dedicated cloud Multi-Zone-Region. However, it should be the customer's choice whether to extend such localisation requirements also to meta-data and cloud service derived data. Additionally, the latest draft is a result of the efforts to reach a workable solution to address the different needs and priorities of the European Member States regarding their competencies national security. Finally, users should have access to clear and transparent information regarding where data is being processed. However, the inclusion of sovereignty requirements within the text would be incompatible with the idea that existing customers would expect the highest security applied to the cloud services that CSPs provide to them and yet CSPs cannot certify against the highest assurance levels of EUCS.

The EU needs a cybersecurity certification scheme that leverages existing and internationally recognised cybersecurity standards to foster global interoperability and to reduce unnecessary compliance burdens for businesses. The deletion of the majority of the politically driven sovereignty requirements (EU HQ) in Annex I of the latest draft is an important decision by the European Union Agency for Cybersecurity (ENISA) that will facilitate a certification scheme for Europe that will be widely adopted, meaningfully raising the cybersecurity baseline for European industries. However, the 'primacy of EU law' criteria that remain in the latest draft run counter to industry practice resulting in a restrictive business environment for third-country cloud users within the EU. Once the European Cybersecurity Certification Group (ECCG) and ENISA conclude their work on the draft scheme, the European Commission should facilitate a transparent process for the adoption of the respective Implementing Act, including meaningful engagement with the industry.

Focus on technical measures and non-technical requirements

The EUCS framework should prioritise robust technical security measures to mitigate cyber threats and ensure service resilience. We understand that the latest ENISA draft does not include the so-called PUA-criteria (Protection of European Data Against Unlawful Access), other than maintaining the 'primacy of EU law' criteria. As highlighted by numerous industry associations, cloud users as well as Member State representatives over the last years, the inclusion of these criteria would create unnecessary complexities and potentially hinder the adoption of secure cloud services. The European Commission should ensure the final Implementing Act reflects the results of the EUCS negotiations and excludes the PUA-criteria including the restrictive contractual proposals discussed in the following chapter of this paper. Instead, the focus should remain on fostering a regulatory

[1] https://www.amchameu.eu/position-papers/cybersecurity-certification-scheme-cloud-services-eucs

environment that promotes innovation, facilitates cross-border data flows and strengthens the overall cybersecurity posture of the EU. This approach can help reset the discussion on sovereignty, moving it from a technical level to a political one. This will allow Member States and the new European Commission to consider digital sovereignty in a new light, focusing on how trust mechanisms and cooperation with strategic allies can actually strengthen it, while preventing cloud service providers headquartered in 'adversarial' countries from engaging in 'forum shopping' in order to obtain the EUCS 'high' trust mark. This approach will not only enhance the competitiveness of businesses but also bolster the EU's resilience against evolving cyber threats in an increasingly digital landscape.

Further concerns and suggestions to improve the EUCS

Lack of reference to international standards

The lack of reference to international standards such as those developed by ISO/IEC JTC1 SC27 (ISO/IEC 27000 series of standards) is a glaring omission in the latest draft of the EUCS. If proven and widely adopted industry practices are not adopted, there is a serious risk of misalignment with such good practice. There are numerous examples of ambiguous requirements and requirements that are not proven to be good practice for improving cybersecurity of cloud services in the current draft EUCS. Instead, the document would be improved through the adoption of the terminology and guidance from ISO/IEC standards, such as ISO/IEC 27001, 27002, 27017, 22123 (eg on the overlap and misalignment of text for definitions, the protection of logs, the use of role-based access control and the penetration testing methods).

Ambiguous and vague requirements

The latest draft contains several requirements that are unclear, too prescriptive, or not consistent with the assurance levels (eg the definition of non-critical data, the use of removable media, the justification of the evaluation level and the management of conflicting roles). The text contains numerous references to the 'state of the art', a term that is rather unclear. State of the art is not always proven and widely adopted practice. A more appropriate term to be used throughout the text would be 'industry best practice'. Ambiguous, vague and inconsistent requirements will potentially lead to issues with certification and testing against such requirements, and create challenges for conformity assessment bodies and auditors who are used to international standards. Furthermore, overly prescriptive requirements can cause issues with conformity if the implementation of the cloud service is different to how the requirement expects the cloud service to function (eg the configuration of data centres).

Concerns over 'primacy of EU law' criteria

The latest EUCS proposal maintains 'primacy of EU law' contractual requirements for the basic, substantial and high assurance levels. The application of contractual requirements to all assurance levels may impact the ability of third-country based companies to utilise cloud services in the EU. Third-country companies often contract according to the legal systems of their home jurisdictions. Requiring cloud contracts to 'only' follow the law of an EU Member State do not reflect contractual practice in certain situations and may result in changes to existing operational practices. Cloud contracts are typically enterprise-wide, framework agreements for services that are consumed across a companies' affiliates within its corporate group. Maintaining the 'primacy of EU law' requirements will therefore result in the EUCS being considered as not suitable by third country companies or increase the contractual complexity involved in utilising cloud services within the EU. Therefore, all primacy of EU law requirements as related to contracts should be deleted from the EUCS.

Conclusion

A technical, standards-based EUCS that is achieved through open consultations and excluding non-technical criteria, will best serve the interests of businesses, citizens and the European economy as a whole. While the gradual removal of sovereignty requirements within the latest draft text is a step in the right direction, the continued inclusion of contractual sovereignty requirements will materially impinge the ability of US, and other non-EU, cloud users to operate within the EU. Contractual sovereignty proposals should be removed from the final EUCS text. Mindful of the sovereign interests of Member States, they should ensure a consistent application of the EUCS across Europe after its finalisation. This will improve interoperability of cloud services across the Union and avoid complexity for businesses operating internationally. Member States should avoid a fragmented landscape of parallel assertion instruments for EUCS, which would continue to discriminate against non-European technology providers to the detriment of European industries and consumers.