June 2024

EUCS: Ensuring full transparency and cybersecurity for European cloud users' data

The negotiations on the EU Cybersecurity Certification Scheme for Cloud Services (EUCS), that have been stalled for a significant period, appear to be coming to a resolution. Ahead of the ENISA Cybersecurity Certification Conference in April, a new draft candidate scheme has been shared that represents a return to technical cybersecurity requirements.

As the financial services industry, we welcome the improvements made in the latest version of the draft EUCS scheme. With the removal of most sovereignty requirements, the latest draft will introduce further transparency for cloud service users, while maintaining open market access and free provider choice. The efforts made to address the widespread concerns over the inclusion of political and sovereignty requirements within the technical scheme are a clear positive step forward to ensure that the focus remains on cybersecurity safeguards and the operational resilience of European businesses. As highlighted in earlier statements, we believe that cybersecurity certification should facilitate this by helping companies make informed choices based on the assurance that cloud providers meet relevant cybersecurity standards.

We encourage the European Cybersecurity Certification Group to reach consensus regarding the removal of sovereignty requirements. As the EU financial sector, we strongly support a uniform cybersecurity certification as it would facilitate the uptake of cloud adoption in the EU financial services sector. Subsequently, we would like to reiterate the benefits of a harmonised technical scheme in line with the objectives and the mandate given by the Cybersecurity Act.

1. **Differentiate between data protection and cybersecurity:** The objective of the EUCS is to ensure that cloud services meet a minimum set of security and trust criteria throughout the EU to facilitate the resilience of its networks and information systems. As clearly stated by ENISA, the EUCS is not intended to ensure compliance with data protection requirements. In light of the already complex regulatory landscape, we would like to highlight that the Data Act, the Data Governance Act and the General Data Protection Regulation (GDPR) already address questions of data access without resorting to sovereignty requirements.

2. **Ensure users' clarity and transparency:** Stripping out sovereignty requirements from the certification scheme will, in fact, increase transparency. Previous versions of the EUCS included sovereignty requirements mostly in the highest assurance level. This could create the misperception that locally based providers are by design more secure than those providers based or headquartered in third countries. Yet, certain providers could have been excluded from obtaining the highest assurance level simply because of their origin – before any assessment of their technical security. It is still important to ensure that customers have all relevant information on data storage, locations and applicable laws.

3. **Ensure competitiveness and growth of the European cloud ecosystem:** One of the reasons for the strong reliance of EU firms on non-EU cloud providers is the market-leading position of U.S. providers, especially in the Infrastructure-as-a-Service and Platform-as-a-Service sector, including their scale and the ability to service clients on a global level. The focus should therefore be on the creation of an environment that increases competition and choice. Excluding non-EU providers via strict localisation requirements for operations, headquarters or contracts will not have this effect: Other jurisdictions will follow suit, creating new barriers for EU providers to service clients outside the EU. And even without retaliation measures, EU providers will face disadvantages when they try to scale their business outside the EU if their contracts have to be exclusively governed by the law of an EU member state. We note that contractual requirements remain in the draft and we support their removal.

We understand that the negotiations on EUCS and potential sovereignty requirements are embedded in the broader discussions on achieving strategic autonomy and competitiveness and take place in a time of heightened geopolitical uncertainty. And we second the importance of those discussions. However, it is essential that those highly political conversations take place in the appropriate political fora and allow for adequate involvement of affected stakeholders from society and industry and are not pushed to technical standards.

AFME:

Marcus Corry - Marcus.Corry@afme.eu

EPIF:

Nickolas Reinhardt - Nickolas.reinhardt@aforeconsulting.eu

Beatriz Barbieri – Beatriz.barbieri@aforeconsulting.eu

Insurance Europe:

Arthur Hilliard - Hilliard@insuranceeurope.eu