POSITION PAPER

# EUROPEAN CYBERSECURITY CERTIFICATION SCHEME FOR CLOUD SERVICES (“EUCS”)

November 28, 2023

The American Chamber of Commerce in Belgium, the voice of international business in Belgium, strives for a positive business environment that encourages (continued) investment and sustainable growth.

In today’s world, where cyberattacks have become part of the arsenal in geopolitical conflicts and can be sophisticated and persistent, cybersecurity is more important than ever. As threats against networked systems are dynamic, cybersecurity must never be static, and constant efforts are needed to improve how digital systems are protected.

Therefore, our members have welcomed the 2019 Cybersecurity Act, which grants, the European Union Agency for Cybersecurity (ENISA) more powers to address cyberattacks and creates a pan-European Cybersecurity Certification Scheme for Cloud Services (“EUCS”).

In essence, cybersecurity certification is crucial for organizations to assess and procure services that best fit their cybersecurity needs, and our members hold and rely on numerous cybersecurity certifications in various geographies, thereby allowing them to provide or choose cloud services according to the sensitivity of certain data and criticality of specific systems.

A common cybersecurity certification framework based on international standards allows for better harmonization at European level in several ways that benefit the market:

- First, due to the principle of mutual recognition, EU-level certification is more time- and cost-effective because a company certified in one Member State is deemed certified in all other 26 Member States and therefore automatically gets market access and opportunities to expand; and
- Second, it is easier for regulators to assess conformity of products and services against legislation or other policies when rules are harmonized and based on existing, internationally recognized standards.

Therefore, the draft European Cybersecurity Certification Scheme for Cloud Services will, if well calibrated, harmonize Cybersecurity certification on the single market, remove complexities and ultimately ensure streamlined and enhanced cybersecurity across the single market.

To achieve that goal, the EUCS should focus on technical measures to strengthen security and resiliency and should rely on consensus-based international standards that have proven their efficiency by way of broad industry adoption. The latest draft versions of the EUCS do however not meet this objective, and AmCham Belgium has identified several areas of concerns with these drafts, as outlined below.

## Evaluation Levels 3 & 4 and Annex I

- *Sovereignty requirements*

The latest draft of the EUCS still contains sovereignty requirements, previously known as Independence from Non-EU Laws. These requirements, which apply to Evaluation Level 4 ("EL4") and are incorporated in Annex I titled 'Protection of European Data against Unlawful Access' (PUA), cause, among other issues, discriminatory global headquarters and ownership requirements.

The sovereignty requirements apply to a very wide range of data and cloud services, since EL4 covers "data of particular sensitivity (personal or not), the breach of which is likely to result in" issues with (i) public order, (ii) public safety; (iii) human life or health, or (iv) the protection of IP[1].

In the "Application to evaluation levels", the draft EUCS also lists the following categories of data as being in the scope of EL4: "data whose breach could reasonably be expected to cause serious injury, for example, loss of reputation or competitive advantage, or to cause extremely grave injury, for example, loss of life"[2]. A literal interpretation of EL4 as currently drafted would mean that it is potentially applicable to most if not all companies active in Belgium.

Due to concerns on too vague and broad scope, this has been limited slightly in the August draft, however the scope continues to cover intellectual property, public health, public order and newly data whose breach can result in loss of reputation or competitive advantage. This means that both the lack of legal clarity, as well as the sweeping nature of the scope continue to be problematic. This two-tiered approach to EL3 and 4, not only makes the scope of EL4 very confusing but also extremely broad.

Accordingly, we foresee that US headquartered cloud services will be subject to EL4, first because of the broad categories of data in scope of EL4 (for instance, all data protected by intellectual property rights or that can cause issues with reputation), but also because the vagueness of the EL4 description makes it difficult for organizations to determine precisely which digital systems require EL4 certification. These organizations would hence need to use the cautious approach and apply EL4 throughout many of their digital systems, seeking providers with EL4 certification for most cloud services they procure.

Thus, even though the data localization requirements have been moved from EL3 to EL4 in the recent August draft, the global headquarters and ownership requirements and vague scope of EL4 mean that the issues with these requirements highlighted below remain unchanged. Last, the addition of EL4 in the new EUCS draft creates a further layer of complexity and does not conform with article 52 of the EU Cybersecurity Act (CSA), which provides for three assurance levels.

- *Data localization requirements*

As part of the contested sovereignty requirements, Annex I also contains data localization requirements which form an issue for multinational companies that need international data flows to avoid disruptions to their operations.

While AmCham Belgium believes that any concerns about foreign government access to data or international data transfers should be addressed through multilateral governmental negotiations establishing common baseline expectations, and not by local legislation, regulations like the Data Act,

[1] EUCS, V1.0.335 | AUGUST 2023, p. 24

[2] EUCS, V1.0.335 | AUGUST 2023, p. 30

which will enter into force later this year, address these concerns. Hence a cybersecurity certification scheme, should contain only technical security requirements.

Lastly, and as raised above, even if data localization requirements were moved from EL3 to EL4 – the overly broad scope of EL4 does not really change the scope of the requirement, and certainly does not address the main issue with data localization requirements, which hamper international operations.

## Risks raised by the current version of the EUCS

Based on the concerns outlined above, AmCham Belgium cautions against adopting the EUCS with sovereignty requirements. The significant barriers to entry for non-EU headquartered companies and EU companies with international/global operations and investments will limit competition in the cloud market. This risks not only raising the cost of cloud services, but also limiting the choice of trusted technology partners for European businesses. It could also considerably limit the market uptake of certification and delay the digitization of EU services and processes beneficial for EU citizens and businesses.

A recent study by ECIPE[3] also concludes that "*smaller EU countries would be disproportionately impacted by GDP losses compared to larger countries. In the short-term, small EU countries that are characterized by high-value-added production, including digital and digitally enabled services, and which rely heavily on imported ICT services, show the largest relative losses in annual GDP.*"

Source: The Economic Impacts of the Proposed EUCS Exclusionary Requirements: Estimates for EU Member States | (ecipe.org)

Furthermore, according to AmCham Belgium, market access limitations need the application of strategies other than a cybersecurity certification program constituted by means of an Implementing Act of the European Commission. Such schemes, which are not debated through democratic lawmaking procedures, should only contain technical cybersecurity requirements.

Furthermore, creating digital isolationism will 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.

Another risk is that other jurisdictions would seek to introduce similar requirements, thereby limiting European companies' business expansion opportunities to non-EU markets. For instance, the US FedRAMP regime (Federal Risk and Authorization Management Program) currently only focuses on the technicalities of cloud cybersecurity, without imposing equivalent sovereignty measures.

[3] https://ecipe.org/publications/eucs-immunity-requirements-economic-impacts/- p. 4

## A Belgian version of the scheme raises multiple questions

AmCham Belgium would also like to caution against a Belgian alternative to the scheme. Due to the very nature of such a scheme, designed in accordance with the Cybersecurity Act as a harmonized framework recognized across all Member States, national alternatives are not viable.

We do not see how the Belgian scheme will be recognized across borders if data protected by IP rights or raising competitive advantages are subject to EL4 in certain Member States, while this is not the case in Belgium. Besides, to be compliant, companies operating across several countries may have to choose the most conservative approach and apply EL4 in all the Member States where they operate.

Moreover, how would an entity certifying under the Belgian alternative either be able to export its cloud services to other countries or use the data which is subject to certification in other Member States?

## AmCham Belgium urges Belgium to avoid the consequences of the scheme

For all the reasons outlined above, AmCham Belgium urges the Belgian government, and all Belgian stakeholders involved in the discussions on the EUCS, to defend an open and competitive cloud services market, where customers can continue to benefit from competitive prices and the quality of service that result from a vast choice of providers and services. More generally, we plead to avoid digital isolationism, resulting in a market deprived from its most innovative cloud products and services.

As a result, AmCham Belgium urges Belgium to be vocal and strongly oppose the requirements of Annex I, as these would lead to severe negative consequences on the usage of cloud services and the uptake of cloud services in Belgium (and, more broadly, in Europe).

* * *

## About AmCham Belgium

Founded in 1948, the American Chamber of Commerce in Belgium (AmCham Belgium) is a dynamic non-profit organization dedicated to improving business and investment opportunities for the US-Belgian business community. Supported by more than 400 member companies, AmCham Belgium plays a pivotal role in an evolving business environment by focusing on three key areas: advocacy, networking, and knowledge-sharing. To learn more about AmCham Belgium, visit www.amcham.be.