# Position Paper

## European Cybersecurity Certification Scheme for Cloud Services (EUCS)

June 2023

**Executive Summary**

This paper builds on AFME's views, as set out in the March 2023 position paper, regarding the sovereignty (immunity to non-EU law) requirements included within the draft EUCS. Despite recent public messaging, we continue to be highly concerned that the sovereignty requirements remain substantively in place, capturing an expansive level of data and posing considerable risk to the EU's capital market innovativeness, resilience and competitiveness. This is a highly disappointing scenario, given that the scheme itself, as a technical measure aimed at enhancing cyber security standards, would have received fulsome industry support in the absence of these political considerations that will undermine the EUCS' original objectives. There are a number of horizontal regulatory proposals where industry would otherwise be calling for the application of the EUCS, but this is not possible with the sovereignty provisions as retained.

### The latest version of the scheme shows little meaningful revision of the sovereignty measures

Despite various member states voicing concern over the sovereignty elements of the proposed EUCS, it is AFME's understanding that the latest version retains several substantive localisation requirements:

- Contracts between Cloud Service Providers (CSPs) and Cloud Service Customers (CSCs) will be governed and construed by EU law, with CSPs additionally obligated to identify potential extra-territorial application of non-EU laws
- The cloud service is to be operated and maintained from the EU, with all CSC data stored and processed inside the EU
- Only employees based in the EU to be permitted access to CSC data, whether direct or indirect
- CSPs to be required to locate their global headquarters within the EU, if they are handling "sensitive" data

While all the above requirements collectively relate only to the 'Highest' category of assurance (via the newly proposed assurance level High+ / CS-EL 4), the first point applies to all categories, and half of the requirements apply to the lower CS-EL 3 category. The latter (CS-EL 3) is regarded as suitable for all cloud services who need specific security requirements (for mission-critical data and systems), which could encompass a broad array of entities, going far beyond the realms of defence and national security. Similarly, while the High+ / CS-EL 4 category is restricted to sensitive cloud services, the expanse of data defined as 'sensitive' is incredibly broad and open to interpretation, encompassing data related to public order, public safety, human life/health, as well as trade secrets, including production methods, economic and financial information, regardless of whether it is personal data or not. Other terminology used, such as "data related to the protection of privacy" is very vague und could include all personal data.

The current EUCS draft continues therefore to retain far-reaching sovereignty requirements in Annex J, with industry concerns over the impact on operational resilience, market choice and digital innovation still very much alive. Further, as acknowledged by ENISA in the latest draft, the above proposals require for their

evaluation competences that are not typically available to Cybersecurity Conformity Assessment Bodies, and are reliant upon engagement with a designated government authority. This underlines AFME's previous concerns that a technical implementing measure is not the appropriate procedural tool for such significant policy discussions.

**Missed opportunity for cybersecurity standards**

AFME strongly encourages the Commission to remove the sovereignty requirements from the scheme. We do so, in part because the scheme would otherwise represent a welcome technical measure which could help bolster cyber security standards across the EU. With a number of ongoing horizontal initiatives, for example as with DG-CNECT's proposed Cyber Resilience Act, industry would support the wider application of the EUCS, had the sovereignty measures not caused such concern. With many of these horizontal proposals, the incorporation of the EUCS would bring technical rigour to a wider policy proposal.

More broadly, we remain concerned about the potential of the sovereignty requirements to undermine the EUCS through incompatibility with the EU's WTO commitments. It is our understanding that the Commission has conducted a legal analysis of the proposed EUCS standards, and we call on officials to publish and engage with industry in addressing these concerns.

AFME remains available to discuss in further detail the views from members and would be happy to organise a follow-up meeting.

**AFME Contacts**


Andrew Harvey
andrew.harvey@afme.eu
+44 (0)20 3828 2694

Marcus Corry
marcus.corry@afme.eu
+44 (0)20 3828 2739

Stefano Mazzocchi
Stefano.mazzocchi@afme.eu
+32 2 8835546