Position Paper

European Cybersecurity Certification Scheme for Cloud Services (EUCS) – Solutions on the Issue of Independence to Non-EU Law

13 March 2023

Executive Summary

This paper summarises AFME's views on the ongoing Member State discussion on the digital sovereignty requirements under EUCS. In particular, we are aware of the "Joint document: alternative solutions regarding the issue of independence to non-EU law in the context of EUCS" ("*INL Non-paper*"). We remain concerned that (1) digital sovereignty issues are too significant to be addressed under the implementing act procedure for technical security measures and (2) that none of the options in the INL Non-paper offer an effective solution for the concerns raised, a comprehensive impact assessment, or even acknowledgement of potential consequences. Accordingly, we propose high-level principles that should be taken into account when addressing these issues.

Process Concerns

The EUCS was originally intended to be a technical scheme to achieve a common security assurance framework for the EU, whilst maintaining EU competitiveness and avoiding costly localisation of operations and technology. Per the European Cybersecurity Act (CSA)[1] mandate, EUCS is in the form of an implementing act, meant for technical requirements, rather than primary legislation that sets and pursues political goals. However, the digital sovereignty elements under discussion (i.e. on storage and processing of data; access restrictions; jurisdiction of contracts; company incorporation and governance; and provision of non-EU law risk assessments), as well as the implementation methods presented in the INL Non-paper, represent significant new requirements that go beyond the remit of an implementing act. This is particularly concerning as the examination procedure under Regulation (EU) No 182/2011[2] that the Commission is mandated to follow for the purpose of the adoption of an implementing act under the CSA does not provide for any transparency in the process nor for any formal industry consultation - and therefore any cost-benefit analysis or political scrutiny. Furthermore, since the (so far, only) public consultation conducted by ENISA in 2021[3], substantive elements of the drafts have changed, and the INL Non-paper is also not publicly available, which further reduces the transparency.

Additionally, we wish to highlight that the INL Non-paper does not sufficiently detail the new digital sovereignty requirements, or note any prioritisation, instead focusing on how the new requirements could be achieved. This is a substantial concern, since the nature of the measures should in fact inform the implementation method. Providing meaningful industry input into the discussion is also challenging without this crucial information.

We understand that these digital sovereignty concerns may be driven by critical areas such as defence and national security. However, the introduction of any such requirements should be done in a very targeted way and is already, in parts, undertaken on national level. Their inclusion into a horizontal framework, the application of which may easily be extended to non-military sectors, seems disproportionate to their aim.

[1] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[2] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32011R0182
[3] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Association for Financial Markets in Europe
London Office: 39th Floor, 25 Canada Square, London E14 5LQ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 883 5540
Frankfurt Office: Neue Mainzer Straße 75, 60311 Frankfurt am Main T:+ 49 (0)69 710 456 660
www.afme.eu

Therefore, while we understand that some stakeholders wish to develop EU digital sovereignty requirements, we do not believe EUCS is the appropriate means for this.

Application to Financial Services

Under Article 4 of the Network and Information Security Directive (NIS 2)[4], sector-specific legislation ("*lex specialis*") may take precedence over the NIS. For financial services, this would be the Digital Operational Resilience Act (DORA)[5], which sets out detailed requirements for a broad range of European financial entities concerning the management of information and communication technology (ICT) risks, including a comprehensive framework for the management of third-party ICT risks.

One of the key elements of DORA is an introduction of the oversight framework for the designated "Critical Third Parties" (which may include Cloud Service Providers), that is designed to cover also such Critical Third Parties that are located in third-countries. Importantly, whilst DORA requires that a designated Critical Third Party that is based in a third-country will have to establish a subsidiary in the EU, it also explicitly acknowledges that ICT services can be provided to EU-based financial entities by Critical Third Parties established in third-countries without the need to locate their operations in the EU (DORA recital 82: "*The requirement to set up a subsidiary in the Union should not prevent the critical ICT third-party service provider from supplying ICT services and related technical support from facilities and infrastructure located outside the Union. This Regulation does not impose a data localisation obligation as it does not require data storage or processing to be undertaken in the Union*").

In this context, the currently contemplated EUCS framework, and in particular the additional digital sovereignty elements, are contradictory to the co-legislators' intentions reflected in DORA. This is especially concerning as the CSA can enforce that certain sectors use only providers with the 'high' assurance level and we expect that this is likely to apply to financial services. For the purpose of ensuring undisrupted access by European financial entities to ICT services provided by service providers established outside the EU, we would strongly encourage that the future EUCS follows the DORA approach.

Possible Consequences for Financial Services

Financial services is a global, highly regulated, technologically advanced industry. Cloud adoption is steadily increasing; it has been estimated that the financial services cloud market will be worth $101.71bn by 2030[6]. Cloud adoption is a way to improve capacity, resilience, client experience and cost efficiency[7].

Yet the introduction of restrictive digital sovereignty measures will adversely impact innovation, agility and resilience in EU financial services. If the regulatory environment becomes too cumbersome, investment will reduce and the cloud market will become less competitive, impacting consumers. Financial institutions will also be restricted from accessing third party systems and services that have already migrated, or were designed as cloud native.

Additionally, a trend towards localisation will result in financial institutions needing to replicate or duplicate operations and technology services in specific locations, limiting economies of scale and increasing operational risk, or even in financial institutions withdrawing from cloud migration plans, leaving infrastructure and services on-premise.[8] This would cut across calls from financial regulators for financial institutions to focus on building resilience and transitioning away from complex legacy systems.[9]

[4] https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[5] https://eur-lex.europa.eu/eli/reg/2022/2554/oj
[6] https://www.prnewswire.com/news-releases/finance-cloud-market-to-be-worth-101-71-billion-by-2030-grand-view-research-inc-301616196.html
[7] https://www.afme.eu/Publications/Reports/Details/The-Adoption-of-Public-Cloud-Computing-in-Capital-Markets
[8] https://www.afme.eu/publications/reports/details/State-of-Cloud--Adoption-in-Europe-Preparing-the-path-for-cloud--as-a-critical-third-party-solution
[9] https://www.bankingsupervision.europa.eu/press/speeches/date/2023/html/ssm.sp230208~4ee762ce05.en.html;
https://www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl190213_4.en.html

AFME Proposed Principles

As above, we do not support the inclusion of digital sovereignty requirements within the EUCS. However, should digital sovereignty and ways to achieve it continue to be discussed, we also do not believe that any of the options set out in the INL Non-paper offers an effective solution, particularly as the paper is limited to process rather than content. On that basis, we propose the following principles to consider when developing alternative proposed measures:

1. Transparent: given the significance of digital sovereignty, measures should follow the correct legislative process, with broad and transparent consultation with all affected industries;
2. Outcomes-focused: measures should target specific risks identified (e.g. unlawful data access) and be designed to increase operational resilience, rather than broadly imposing an unnecessary compliance burden on industry or restricting access to key third country services;
3. Efficient: measures should avoid creating bottlenecks (for example with extensive regulatory approval processes) that will hinder the overall adoption of cloud technology within the EU;
4. Subject to economic impact assessment: as noted in the INL Non-paper, measures should be preceded by economic impact assessments, involving all affected industries;
5. Legally certain: measures should be agreed at the outset, be proportional and subject to review only at appropriate intervals, giving industry some certainty over their scope at least for the medium term, in order to attract investment; and
6. Globally minded: measures should align to global data and technology standards, rather than increasing regional compliance costs for industry, and should not breach the EU's WTO commitments.

AFME Contacts

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

Fiona Willis
fiona.willis@afme.eu
+44 (0)20 3828 2739

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