IRSG
INTERNATIONAL
REGULATORY
STRATEGY GROUP

IRSG letter – EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

The International Regulatory Strategy Group (IRSG) would like to share its concerns, in line with other industry representatives, on the cloud sovereignty requirements which are currently being discussed as a key element of the EU Cybersecurity Certification Scheme for Cloud Services (EUCS).

The EUCS was originally intended to be a technical scheme to achieve a common cloud security assurance framework for the EU, whilst maintaining EU competitiveness and avoiding costly localisation of operations and technology. Under the European Cybersecurity Act (CSA) mandate, EUCS ought to take the form of an implementing measure, intended for technical requirements, rather than introducing a major new policy departure with consequences extending far beyond the EU's jurisdiction.

However, the digital sovereignty elements under discussion, as well as the implementation methods presented in the "Joint document: alternative solutions regarding the issue of independence from non-EU law (INL) in the context of EUCS" (INL Non-paper), represent significant new requirements that amount to a substantive policy change with global effects.

Cloud sovereignty was rejected by the EU when the EU Council decided in 2022 against sovereignty measures in adopting Regulation (EU) 2022/2554 (the Digital Operational Resilience Act - DORA). DORA envisages a direct oversight regime for critical Cloud Service Providers (CSPs) instead of imposing discriminatory restrictions, localisation obligations and company ownership requirements on non-EU technology providers. The UK and the US appear to favour types of approach essentially similar to that envisaged under DORA i.e. not requiring localisation.

The new proposals revisit this key EU policy decision. Trading partners would expect such a major change to EU policy to be made at the highest EU decision-taking level with appropriate transparency and deliberation. It would be preferable – and far more reassuring for the EU's trade partners - for the proposals on cloud sovereignty to be considered not simply as draft ENISA technical requirements, and instead to be properly debated by a broad range of EU policymakers. Such an approach would allow the proposals, like all major proposed EU policy changes, to be subject to the EU's standard cost-benefit analysis.

We agree with the concerns outlined in the AFME position paper published in April 2023 and the potential consequences for financial services highlighted in the paper. We also agree that alternative measures which might be developed should be transparent, outcomes-focused, efficient, subject to economic impact assessment, legally certain and consciously framed with an eye to their wider global consequences.

We would also like to highlight the IRSG reports on Data localisation and international data transfers, in which we set out the challenges data localisation brings for our sector and our economies as a whole, and present our recommendations on how alternative measures could

potentially better address the concerns of both national governments and regulators.

The proposed cloud sovereignty policy would weaken cybersecurity and resilience while harming the EU's international standing. It is unclear whether they would enhance the EU's economic competitiveness. In the IRSG's view, the best way to protect EU citizens from cyberthreats is not to impose a discriminatory cloud sovereignty regime but for the EU to make full use of the policy tools provided by DORA, the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), and GDPR data adequacy.