FESE response to the Commission *Have Your Say* Consultation on the Cloud and AI Development Act

10th November 2026

Q1: Feedback (*4000 characters limit*)

We welcome the EC's ambition to strengthen the EU cloud computing capacity and reduce strategic dependencies. The Cloud and AI Development Act (CADA) addresses a genuine challenge. Certain provisions, however, notably the pathway for extending impact assessments and possible procurement restrictions to the private sector under Art. 31, require careful reconsideration.

Art. 31(3) CADA empowers the EC, by delegated act, to require private-sector entities in sectors of high criticality to conduct impact assessments of their cloud services and adopt risk-mitigation measures. Triggering conditions, such as "*specific circumstances*" and "*where duly justified*" lack precise legal definition, granting the EC broad discretion to activate these powers. This open-ended drafting leaves the door open to delegated action, creating legal uncertainty for entities that must plan infrastructure investments years in advance. An unspecified but potentially far-reaching power to impose mandatory risk-mitigation measures introduces the risk that contracts concluded today may require retrospective amendment. This uncertainty weakens the negotiating position of European entities vis-a-vis cloud providers. Scaling cloud and AI adoption requires investment predictability and the ability to conclude long-term contracts, not the looming threat of procurement restrictions.

It is essential to recognise that the protection of sensitive financial sector data is already comprehensively addressed through binding sectoral legislation. DORA Art. 9(2) requires financial entities to *develop, document, and implement dedicated policies on encryption and cryptographic controls, covering data at rest, in transit, and in use*. Art. 9(4)(d) mandates *strong authentication mechanisms and dedicated protection measures for cryptographic keys* across their entire lifecycle. The accompanying RTS under Art. 6 specify concrete requirements for algorithm selection, key management, and audit trails. In parallel, NIS2 Art. 21 obliges essential and important entities to adopt proporti*onate technical, operational, and organisational cybersecurity measures* following an all-hazards approach, explicitly covering supply chain security, encryption policies, and access control. Cloud computing service providers are themselves classified as essential entities under NIS2, subjecting them directly to these obligations.

Financial entities already subject to DORA should therefore be explicitly excluded from mitigation measures adopted under Art. 31(2). We also recommend clarifying that delegated acts adopted under Art. 31(3) shall not apply to financial entities within DORA's scope, together with a recital recognising DORA as the sector-specific Union framework for these entities.

Open-ended risk-mitigation measures risk service degradation, concentration in fewer providers, and costly contract renegotiations that would consume internal resources for years based on political intervention instead of technological advancement. The European cloud market does not currently offer services at the scale and performance levels that critical FMIs demand. **We therefore caution against introducing broader mandatory**

private-sector obligations or procurement restrictions. Any such measures would impose severe economic consequences and impair industry's ability to innovate. Restricting available business opportunities, while competitors in the US, the UK, and other markets retain full flexibility, weakens Europe's position when the SIU agenda calls for more attractive capital markets.

Lastly, decisions with the potential to reshape cloud procurement for entire industries, including critical financial infrastructure, warrant full co-legislator scrutiny. The Regulation should define objective criteria that must be satisfied before such delegated acts are adopted and ensure that existing sectoral regulatory frameworks are recognised as mitigating factors, instead of a simple consultation with the Member States.