European Association of CCP Clearing Houses

Brussels, 10th November 2026

EACH High-Level Feedback – EU Cloud and AI Development Act (CADA)

The European Association of CCP Clearing Houses (EACH) appreciates the opportunity to provide input on the Cloud and AI Development Act (CADA)[1]. We have focused our response on Article 31(3).

Article 31(3) requires, via delegated act, that private-sector entities in highly critical sectors conduct mandatory impact assessments of their cloud services and adopt risk-mitigation measures, and gives the European Commission broad discretion to activate these powers due conditions like "specific circumstances" and "where duly justified". This risks creating uncertainty for entities that must plan years ahead, and implies the potential renegotiation of existing contracts, which in turn negatively affects existing relationships and also the position of European entities globally.

To this end, we would emphasise that Europe's financial sector is already well prepared here due to the existing frameworks, for example the Digital and Operational Resilience Act (DORA)[2] and NIS2[3]:

- 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.
- DORA's RTS 2024/1774 Art. 6 specifies concrete requirements for algorithm selection, key management, and audit trails. Also, before contracting, DORA already requires financial entities to, for instance, (i) assess concentration risk and the provider's substitutability, weigh alternative providers, consider subcontracting chains (Arts 28(4)(c), 29); (ii) maintain documented, tested and periodically reviewed exit plans with identified alternatives and appropriate transition arrangements (Art 28(8)); (iii) have in place contracts that provide termination rights, return of data and a mandatory transition period (Art 30(2)(d), (h), 30(3)(f)). Substitutability and exit planning are recorded in the register of information, and supervisors can require suspension or termination of arrangements with critical providers (Art 42).
- NIS2 Art. 21 in parallel obliges essential and important entities to adopt proporti*onate technical, operational, and organizational 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.

Imposing additional open-ended risk-mitigation measures on entities already subject to comprehensive operational resilience and cybersecurity requirements risks service degradation, concentration in fewer providers, costly contract renegotiations, and overall higher costs to the entire market without a corresponding security gain. The European cloud market does not currently offer services at the scale,

[1] https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

redundancy, and performance levels that critical FMIs demand. Measures that further restrict the range of cloud solutions available to critical FMIs could therefore increase concentration risk and constrain their ability to select services that meet their operational resilience requirements. More broadly, restricting the cloud solutions available to European entities could weaken their competitiveness at a time when the Savings and Investments Union agenda seeks to strengthen the attractiveness and competitiveness of EU capital markets. Any powers with the potential to reshape cloud procurement across highly critical sectors, including critical financial infrastructure, should therefore be subject to clear and proportionate conditions for activation and appropriate safeguards and scrutiny. Rather than placing the burden on the demand side, this work should remain proportionate and risk-based, as well as seek to complement existing frameworks (e.g. DORA, NIS2), avoid duplicative requirements, whilst investing in Europe's supply side potential.

About EACH

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 19 members from 15 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

Contact EACH

Media Team
+32(0)22061260
info@eachccp.eu