Have Your Say: AFME response

EU Cloud and AI Development Act (CADA)

2 November 2026

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on the CADA Have Your Say consultation. The Association for Financial Markets in Europe (AFME) is the voice of the leading banks in Europe's financial markets, providing expertise across a broad range of regulatory and capital markets issues. We represent over 150 leading global and European banks and other significant market players. Our members play a vital role in Europe's financial ecosystem, underwriting around 90% of European corporate and sovereign debt, and 85% of European listed equity capital issuances. Importantly, AFME members are market makers, providing liquidity, which is essential for ensuring financial markets can function efficiently. We also represent law firms and other associate members which advise market participants and support AFME's legal and regulatory initiatives.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

Summary

- The financial sector supports the development of a competitive EU-based cloud computing services market. As a critical driver of high-growth industries, the sector is well-positioned to support EU advances.
- AFME welcomes the decision of the EU Commission in the proposed Cloud and AI Development Act (CADA) to require public administrations to focus on assured EU providers in the public procurement of critical cloud services.
- Article 31 of CADA has created considerable concern due to the potential far-reaching repercussions of the proposed delegated act. Public procurement instruments do not automatically translate across to private entities, especially given the highly diverse set of sectors in scope, each with differing supply chain complexities. The potential for procurement restrictions on critical private entities risks systemic disruption and the curtailment of market choice and innovation.
- We strongly urge the deletion of Article 31 to maintain CADA's intended focus on public sector procurement reform. Failing that, the provisions in Article 31 should be bolstered through a series of policy and procedural safeguards, with sufficient recognition of existing frameworks within NIS2 critical sectors.

The financial sector supports the development of a competitive EU-based cloud computing services market. As a critical driver of high-growth industries, the sector is well-positioned to support EU advances.

AFME supports the growth of cloud and AI infrastructure capacity in Europe and recognises the benefits that increased competition would bring to a relatively concentrated market, for

Association for Financial Markets in Europe
London Office: Level 10, 20 Churchill Place, London E14 5HJ, 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: c/o SPACES – Regus, First Floor Reception, Große Gallusstraße 16-18, 60312, Frankfurt am Main, Germany T:+ 49 (0)69 710 456 660
www.afme.eu

Company Registration No: 6996678 Registered Office: Level 10, 20 Churchill Place, London E14 5HJ
AFME is registered on the EU Transparency Register, registration number 65110063986-76

both firms and the EU market more broadly. To this end, the financial services sector will continue to voluntarily work with EU providers as a major user of Cloud and AI Services.

Indeed, this is already evident to date in the volume of investment, the number of high-profile partnerships with European providers and the scale of engagement in start-up initiatives. The ECB itself recognised in a 2023 survey that financial services are one of the leading European industries in terms of reliance on Cloud and in driving innovation through the adoption of new technologies.

Yet Europe benefits most when its firms can also access best-in-class global cloud and AI offerings and solutions. The European Commission's communication on Digital Sovereignty recognises the importance of working with trusted international partners and, in light of the developments on Frontier AI, the EC has identified that an immediate priority must be to support critical sectors in adapting to threats this could pose, including by integrating available AI solutions into cybersecurity operations. This also facilitates multi-cloud strategies and access to globally distributed group technology hubs, with geographic and provider diversification in fact strengthening resilience.

AFME welcomes the decision of the EU Commission in the proposed Cloud and AI Development Act (CADA) to require public administrations to focus on assured EU providers in the public procurement of critical cloud services.

Public administrations are uniquely placed to drive this growth, given the localised nature of public data flows and the ability to rely on public procurement tools which are not available to the private sector. The financial services industry welcomes the growth and development of EU providers in response to the implementation of the proposed Articles 29 & 30 of CADA. This is the most appropriate means of unlocking EU growth and should in time create viable market options for sectors such as banking.

However, industry is concerned that private entities, including banks, could be inadvertently brought within the scope of Articles 29 and 30 under the current drafting. Framing these obligations by reference to public sector *activities*, together with the statement in Article 30(3) that contracting authorities include entities acting on their behalf, could unintentionally extend these obligations to the private sector.

Similarly, Recital 66 is based on the premise that requirements applicable to the public sector will tend to naturally extend to the private sector through spillover effects. However, as technology adoption in the private sector is driven by multiple factors, spillover effects should not be assumed to occur automatically. In this regard, the wording of the Recital should be reconsidered to avoid implicit but inaccurate assumptions.

Article 31 of CADA has created considerable concern due to the potential far-reaching repercussions of the proposed delegated act. Public procurement instruments do not automatically translate across to private entities, especially given the highly diverse set of sectors in scope, each with differing supply chain complexities. The potential for procurement restrictions on critical private entities risks systemic disruption and the curtailment of market choice and innovation.

Article 31 establishes a framework through which the European Commission can introduce, with a great degree of discretion, requirements on private entities operating in sectors of high criticality, including financial services:

- Article 31(1) introduces the possibility for private sector entities to carry out voluntary risk assessments similar to the ones that are foreseen for the public sector.

- Article 31(2) confers on the Commission the right to issue guidance specifying the methodology and specific risk mitigation measures. The guidance would apply public procurement-based sovereignty guidance across sectors including water, telecommunications and credit institutions.

- Article 31(3) reserves the right for the European Commission to turn voluntary risk assessments into mandatory requirements via a delegated act.

While we recognise the intent behind Article 31 and the associated reference within Recital 66, it creates serious legal and operational uncertainty that risks undermining confidence for banks operating in the EU market – particularly without sufficient clarity as to the scope, application or interaction of the mandate with existing sectoral regulatory frameworks. Financial services, and especially Capital Markets, are global and cross-border in nature, with sovereignty restrictions – particularly assurance levels 3 and 4 – likely to have a major impact. This would inevitably reverberate across wider industry, given the systemic dependencies at play.

If financial institutions were forced to migrate away from cloud services providers who had failed to achieve the requisite assurance level, this would significantly constrain provider choice in a market where EU cloud offerings do not yet offer comparable scale, performance or technical functionality for complex financial operations. Any prescriptions regarding migration, localisation, provider nationality or ownership conditions should not be part of guidance, but of level 1 legislation. AFME has previously identified a range of risks which would flow from the imposition of such procurement restrictions within financial services, and which are set out in full in an Annex to this paper. These risks would especially affect globally integrated corporate structures, which are necessary for the EU to compete at the global level. This results in group-wide technology, cybersecurity, cloud and AI capabilities delivered across several jurisdictions, with forced fragmentation reducing cyber visibility, duplicating controls and weakening recovery capabilities.

These concerns are exacerbated by the fact that voluntary EU regulatory provisions have in the past become enforced supervisory expectations with a presumption of non-compliance. We are particularly alarmed by several proposals in the other sections of CADA, which could, in theory, be replicated under Article 31:

- Article 29.1(a) states that in identifying which cloud services are in scope of the Regulation, public authorities should focus on those services which "*contribute to the preservation of public order".* This is likely to create significant confusion, as occurred during the previous unsuccessful efforts by policymakers to scope the EUCS (EU Cyber Certification Scheme for Cloud Services) around "sensitive data". Open-ended concepts invite inconsistent national implementation and require exhaustive definitions.

- Annex II of CADA sets out the criteria for the 4 tiers of assured cloud services providers. In the event that financial services were required to use providers with an assurance level of 3 or 4, as part of the referenced mitigation measures, this could significantly restrict market options, despite their criticality to the current scale and pace of Cloud adoption and AI innovation. The annex again provides further detail on the likely impact from such market restrictions.

- The requirement under Article 29.6 for public administrations to complete a migration of Cloud services within 12 months is not seen as technically feasible for sectors such as financial services, with complex ICT supply chains, often bundled into enterprise agreements at the global level. If migration powers are retained, a minimum of 36–60 months would be vital for safe, secure migration within critical environments.

We strongly urge the deletion of Article 31 to maintain the focus on public sector procurement. Failing that, the provisions in Article 31 should be bolstered through a series of policy and procedural safeguards.

CADA's main focus under Title IV is the use of cloud computing services by the public sector in EU member states and this should be maintained. We foresee the transition of EU public administrations to *assured EU providers* to be a major Operations programme, which will require a concentrated drive by policymakers and demand considerable technical resourcing from administrations. To secure traction and boost the chances of successful migration, we would caution against broadening the initial version of CADA to include the private sector. While an assurance level framework for intra-EU procurement may be appropriate for public sector use cases, private sector firms often operate in a fundamentally different environment. European companies with a strong global footprint, or ambitions to expand internationally, need the flexibility to design service landscapes and IT architectures that support customers and business activities across multiple jurisdictions. It is likely that the replication of procurement rules normally reserved for the public sector within such industries would prove challenging and counter-productive in terms of resiliency, if not impractical and unworkable, while serving to unnecessarily increase operational risk. Article 31 would additionally apply across 18 critical sectors, combining sectors with highly international business models, including financial services, air transport, pharmaceuticals and space, despite each maintaining a highly unique supply chain. Rather than risk the delegated act becoming an unwanted distraction from the main thrust of the Regulation, we strongly encourage policymakers to reserve this option for future statutory reviews of CADA, where the lessons learnt by public administrations can be fully assessed prior to any proposal being considered for extending CADA to the private sector. In general, material obligations should be set through the ordinary EU legislative process, not guidance or delegated measures. A measure capable of reshaping critical financial-sector architecture requires full legislative scrutiny, sector consultation and legal safeguards.

If Article 31 is retained, we would urge policymakers to insert clear policy safeguards to avoid any unintended consequences, most notably any delay in Cloud investment as private sector entities wait for sight of the delegated act's requirements. Paramount among these safeguards is protection against any extension leading to duplication and potential conflicts with existing supervisory expectations and sectoral frameworks. Critical entities already conduct comparable risk assessments and implement mitigation measures under existing frameworks including NIS2 and CER. For example, DORA requires financial institutions to assess and manage ICT dependencies, concentration risk, service continuity, subcontracting, data-related risks and exit strategies. Policymakers should carefully assess whether sovereignty-based procurement restrictions could conflict with these frameworks. For example, limiting the pool of eligible providers may concentrate critical services among a small number of cloud providers (with more limited data centre resilience), creating new single points of failure and potentially conflicting with DORA's resiliency objectives.

Specifically, these safeguards should include:

- A specific provision stating that the Commission will only seek to proceed with the delegated act where there is support from a qualified majority of Member States, with any measure time-limited and subject to renewal.

- A prohibition on the delegated act applying in critical sectors where existing sectoral Union regulatory frameworks apply. Any delegated act should demonstrate compatibility with existing sector-specific Union rules and should not inadvertently increase concentration risk or reduce resilience. In the case of financial services, this would avoid any duplication with Regulation (EU) 2022/2554 (DORA). This framework includes robust requirements governing ICT third-party risk management and related contractual safeguards and a special regime for Critical Third Parties. These measures are specifically designed to address risks arising from third-party dependencies, including concentration risk, data location

and processing, supply chain risk management, exit planning, legal and compliance risk. It is also supplemented by technology-specific guidance, such as the European Central Bank's (ECB) cloud outsourcing guide, which already requires cloud resilience solutions targeted at geopolitical risk. Such a prohibition could be facilitated through the EU *lex specialis* procedure, as was successfully deployed to avoid overlap between DORA and NIS2.

- Assurance that any future extension of CADA requirements onto critical private entities should be based on clear, objective and proportionate criteria. In particular, any measures should focus, where justified, on specific activities, functions or use cases that are demonstrably relevant to public security objectives, rather than applying indiscriminately across all institutions in a critical sector.

- Identification of formal industry channels to ensure that affected sectors can highlight operational and technical considerations which should be factored into any remedial measures outlined within the delegated act. The financial sector operates under highly specific technical, regulatory and security constraints. Guidance that pre-determines mandatory measures without drawing on that understanding risks producing requirements that are operationally unworkable or legally inconsistent with established financial sector obligations.

- The incorporation of sectoral bodies and supervisory authorities who are best placed to guide the development of any delegated act, namely the European Central Bank, the ESAs and equivalent competent authorities in the field of financial services.

- Existing certification schemes, standards and audit mechanisms, including those already performed under applicable EU regulatory frameworks, should be recognised and leveraged wherever possible to avoid unnecessary duplication, reduce the operational burden associated with parallel audits, and promote the efficient use of existing assurance mechanisms.

- Adequate transition periods and proportionate implementation timelines should be provided, taking into account the complexity of cloud infrastructures and ongoing ICT transformation programmes.

- An economic impact assessment of sovereignty, localisation, audit and assurance requirements, including their effects on cloud service costs, market competition, financial stability and the total cost of ownership for financial institutions. Transparency should also be ensured regarding compliance costs passed on by cloud providers to customers, and consideration should be given to the need to exempt intra-group arrangements, especially those covered by existing rules such as DORA.

ANNEX:

AFME foresees that any prohibition on choice or imposition of mandatory use of EU cloud providers in financial services would likely result in:

- **Innovation slowdown:** imposing conditions on the procurement of cloud services, particularly if such conditions were to prohibit use of GenAI and AI services provided through hyperscaler platforms, would limit the ease of access to cutting-edge AI tools in the short term. Without these tools, the speed of innovation might be impacted. An obligation to use sovereign solutions would also add significant complexity to European firms operating on a global scale.

- **High cost and delayed time-to-market:** a mandatory requirement to move to service providers with an assurance level of 3 or 4 for certain use cases would be very challenging given the scale of remediation required. There needs to be a consideration of, among other elements, operational risk during migrations, impact on resilience and the specificities of the regulatory business environments. This includes building out the security guardrails, common platforms and connectivity to the cloud environment. For banks operating globally, there is the risk of replicating capabilities that are already available. The complexity and time needed for migrating ultimately depend on the service in question; for example, tailored services take a longer time. Imposing rules on mandatory use of EU cloud providers without considering banks' widespread reliance on incumbent service providers (such as hyperscalers for certain services) and the need to unravel existing supply chains could also require significant cost and time. Any such rules should take into account these factors and permit a proportionate approach should the risks outweigh the benefits. During this time, innovation risks being placed on hold indefinitely while banks wait for European providers to reach the scale required and in order to balance the high-cost impact.

- **Technical integration:** Currently both EU-headquartered and non-EU financial institutions operating in the EU use global platforms in a variety of circumstances, including for crucial services such as cross-border payments, trading, risk analytics, anti-money laundering (AML) and know-your-customer (KYC) systems. These services often utilise non-EU technology providers or are based on-premises and, for certain set-ups, would require parallel operating systems in EU-based cloud service providers (if available or feasible within the specific provider). EU cloud providers' service types, while sometimes similar to those of major global hyperscalers, may present significant technical differences and may require updates to banks' existing infrastructures, which are geared to currently available solutions. Cloud, AI, cybersecurity and technology services provided by an affiliated undertaking should also not be restricted solely because they are delivered cross-border, where the regulated entity demonstrates effective governance, audit access, security, resilience, exit planning and supervisory access.

- **Digital operational resilience risks:** The shift to sovereign Cloud may even have wider negative consequences which counteract the intention of policymakers and supervisors to develop a more secure, robust European market. The ability to rely on cross-border data transfers and multi-jurisdictional back-up facilities is a key element of financial institutions' operational resilience. Restrictions on global AI models can, for example, impair fraud detection, cyber defence, anti-money laundering, software engineering and customer service. Limiting access to providers that are able to offer the necessary capabilities could also reduce the ability of financial institutions to implement effective and credible multi-cloud strategies. Additionally, the requirement for only EU personnel to be engaged for certain assurance levels could detract from broader resiliency strategies, while

widespread market migration to a likely limited number of providers could result in concentration-of-change risk.

- **Restriction of on-premises capabilities:** the Commission needs to carefully consider how to define sovereign solutions. The EU Cloud Sovereignty Criteria for the Commission's own procurement introduce sovereignty criteria that consider a non-EU parent having influence over data as a negative impact on the sovereignty of the cloud service provider. If these were to be taken on board in CADA, all non-EU financial institutions therefore could find that their EU-based on-premises data centres no longer reach the highest sovereignty criteria, substantially impacting the wider IT strategies of non-EU financial institutions.