

EFA Position on the Tech Sovereignty Package

The European Fintech Association (EFA) is a not-for-profit organisation representing fintech companies of all sizes operating across Europe. Its members provide a broad range of innovative and regulated financial services and rely on secure, resilient and interoperable digital infrastructure to serve consumers and businesses throughout the Single Market. EFA engages with EU policymakers to promote a competitive, innovative and well-regulated European fintech ecosystem.

It shares the European Union's objective of strengthening Europe's technological capacity, resilience and security of supply. Achieving that objective will require a framework that expands Europe's capabilities and reduces avoidable dependencies, while preserving the operational flexibility, interoperability and provider choice on which regulated European fintechs rely.

EFA therefore supports the package's emphasis on open source, infrastructure investment and resilience, but considers that targeted changes and clarifications are needed to the proposed Cloud and AI Development Act (CADA). In particular, the framework should remain risk-based, proportionate and coherent with existing sectoral legislation, and should not introduce prescriptive criteria that constrain European firms without a demonstrable resilience or security benefit.

In particular, EFA notes:

1. The **Open Source Strategy is an important step** to place open source at the centre of the EU's tech sovereignty ambitions, and alongside it, open access to data as the complementary lever of European autonomy. **EFA wishes to provide concrete ideas** for possible actions that policymakers could take to achieve the objectives of the initiative.
2. Although its mandatory requirements currently apply to public procurement, **Article 31(3)** would allow elements of the framework to be extended to private entities in high-criticality sectors, including financial-services firms. EFA is concerned that this could create **duplicative obligations** for firms already subject to sector-specific rules and restrict provider choice through criteria based on where technology is developed or manufactured. EFA therefore calls for **Article 31(3) to be deleted**.
3. **CADA's new definition of an "AI agent" introduces a second statutory concept into the acquis alongside the AI Act's** settled definition of an "AI system", creating a risk of interpretive divergence.

We set out all three concerns below, together with our recommendations.

Strong support for the Package's open-source strategy

We particularly welcome the EU Open Source Strategy and its placing of open source at the centre of European technological sovereignty. Open source, interoperability and portability can make a material contribution to European technological resilience by reducing lock-in, broadening access to technology and enabling firms to build, adapt and switch solutions over time.

Open source is not a niche concern; it is critical to commercial software development, including in the regulated sector. [Reports](#) estimate that 96% of commercial codebases contain open-source components. Open source is the backbone of the modern internet and of the financial services that run on it, yet it remains under-recognised in policy and under-supported relative to the physical infrastructure Europe funds as a matter of course.

The Strategy's core aims map directly onto what is needed to support appropriate open-source software adoption in financial services:

- **Procurement reform that lets open source compete fairly in public tenders** - the single most effective lever for reducing vendor lock-in and strengthening genuine provider choice. This is the right way to develop a competitive EU sector: by widening options, not narrowing them.
- **Interoperability and lower switching costs**, which help European fintechs directly and guard against dependency on any single vendor.
- **Long-term sustainability of the open-source projects Europe relies on** - sustainable funding, security attestation and support for maintainers - so that shared infrastructure does not degrade through under-investment.

EFA's Recommendation

EFA encourages the co-legislators to go further where they can: standing technical advisory groups to give policymakers direct access to open-source expertise; proportionate, risk-based and internationally coordinated treatment of open source rather than one-size-fits-all burdens; and regulatory clarity for developers of shared infrastructure.

The open-source strategy and the cloud-sovereignty framework should pull in the same direction. Open source, interoperability and portability are how Europe reduces strategic dependency while preserving choice - pursuing sovereignty by *widening* the field rather than narrowing it. The concern we raise in Section 2 is that certain provisions risk cutting against that logic.

The cloud-sovereignty framework in CADA, its potential extension to private entities, and its provenance orientation

EFA supports the objective of strengthening the resilience, security of cloud services, in line with the EU's digital sovereignty agenda, used by public bodies. However, the CADA framework requires safeguards to ensure that it remains targeted, evidence-based and compatible with the regulatory architecture already governing financial services.

In its current form, the proposal risks extending a public-procurement framework into regulated private sectors through delegated acts, while relying on input-based criteria that may limit the ability of European firms to select, combine and switch secure technologies. European technological sovereignty should increase Europe's capacity to act and innovate; it should not reduce the range of resilient options available to European businesses.

The current framework is, in its mandatory application, appropriately confined to the public sector. Member States and Union entities conduct risk assessments to determine the required assurance level for public-sector activities (Article 29), and contracting authorities must procure at least Union assurance level 1, rising to levels 2 to 4 only where a risk assessment finds the activity to have "public order relevance" (Article 30). This is appropriate for a public procurement framework applied on a case-by-case basis.

Three features, however, warrant attention:

1. **Extension to private entities under Article 31(3).** CADA already provides a route by which the assurance framework may reach the private sector. Under Article 31, non-public-sector entities within NIS2 Annex I may carry out assessments voluntarily (Article 31(1)), the Commission may issue guidance (Article 31(2)), and - critically - the Commission may adopt delegated acts under Article 45 to require such entities in high-criticality sectors to carry out impact assessments and to specify the risk-mitigation measures they "shall" take (Article 31(3)). This could convert a voluntary regime into a mandatory one for private high-criticality entities, which include financial-services firms, by delegated act rather than through the co-legislators. The concern is not the voluntary option; it is the breadth and low threshold of the delegated-act power and the risk of a parallel obligation layered on entities already comprehensively regulated for third-party and resilience risk.

2. **Coherence with DORA.** CADA's own explanatory memorandum states that the proposal “supports the objectives of” the Digital Operational Resilience Act (DORA) and characterises DORA as sector-specific to financial services; Recital 63 expressly identifies data subject to DORA and to NIS2 among the categories the framework covers. DORA already governs ICT third-party and concentration risk for financial entities, including the oversight regime for critical ICT third-party providers, in application since 17 January 2025. Any exercise of the Article 31(3) power in respect of financial entities therefore risks duplicating, or conflicting with, obligations DORA already imposes on the same firms and the same services. We note that CADA's sovereignty framework and DORA are directed at different risks - third-country control and access on the one hand, operational resilience and concentration on the other - and the appropriate response differs accordingly (see recommendations).
3. **A provenance orientation, visible in the award criteria.** The framework's preference for European *origin* over security *outcomes* is visible even in the public-procurement award criteria. Although Article 32 applies only to public procurement by contracting authorities and imposes nothing on private firms, it is instructive as to the drafting mindset: Article 32(2)(d) rightly requires the “Union added value” criterion to be “ancillary and not decisive”, yet Article 32(3) then directs authorities to score technology by where it is “designed or manufactured in the Union” (32(3)(a)), whether it integrates “technologies developed in the Union” (32(3)(b)), and whether the service runs on hardware “designed and/or manufactured in the Union ... to the greatest extent feasible” (32(3)(d)). Provenance criteria of this kind sit in tension with the non-decisiveness safeguard, and - if imported into any private-sector obligation under Article 31(3) - would operate as a *de facto* origin preference, fragmenting the single market in which fintechs exercise their passporting rights without delivering a corresponding resilience gain.

EFA's recommendations

1. **Delete the proposed Article 31(3), granting the Commission delegated-act power.**
2. **Defer to DORA for financial entities.** Consistent with CADA's own memorandum treating DORA as the sector-specific instrument for financial-entity ICT resilience, the framework should defer to DORA for regulated financial entities rather than layer a parallel assurance obligation on the same services. Firms meeting DORA's third-party and resilience obligations should not face a second, sovereignty-driven regime for those same obligations.
3. **Favour outcomes over origin.** Sovereignty and “Union added value” criteria - in Article 32 and in any measure that draws on the assurance framework - should be recast to assess security of supply, continuity and resilience outcomes (as Article 32(3)(c) already does) rather than the design or manufacture origin of the technology.. The framework should preserve the ability of regulated entities to use interoperable, secure and resilient technologies, including through multi-provider and hybrid strategies, while avoiding new fragmentation in the Single Market.
4. **Recognise existing compliance.** Firms meeting the GDPR, the AI Act and DORA should not face duplicative sovereignty obligations for the same services.

The “AI agent” definition in CADA and coherence with the AI Act

CADA introduces a definition of an “AI agent” in Article 2(5):

“an AI system or a coordinated set of AI systems, that can perceive and act upon their environment, with a degree of autonomy, using tools as needed to achieve specific goals and adapt to changing inputs and contexts.”

This sits alongside the AI Act's definition of an “AI system” (Article 3(1) of Regulation (EU) 2024/1689), to which CADA itself cross-refers at Article 2(3). We understand the definition's purpose: Recital 21 and operational objective 6 tie “AI agent” to the Cloud and AI Leadership Initiatives - the sovereign platforms CADA proposes to support for the large-scale deployment and orchestration of AI agents.

EFA supports the development of European capacity for the deployment and orchestration of agentic AI. That industrial objective should, however, be pursued without introducing avoidable legal uncertainty or overlapping concepts into the EU's established AI framework.

Our concern is narrower and is one of *legal coherence*, not of double regulation. Introducing a second, differently-worded statutory definition of an agentic concept into the *acquis* carries two risks. First, *interpretive divergence*: two definitions covering substantially overlapping ground invite uncertainty as to which governs a given system, and as to whether the CADA formulation is intended to mean something different from the AI Act's. Second, *downstream uptake*: a definition coined for the limited purpose of scoping the Leadership Initiatives may be picked up by later instruments or by supervisory practice as the reference concept for "AI agent" in Union law, propagating the divergence beyond CADA's industrial-policy context. For a sector deploying autonomous, tool-using AI in regulated workflows, coherence between CADA and the AI Act on this concept is directly valuable.

EFA's recommendations

1. **Cross-refer, do not restate.** To the extent a reference to agentic AI is needed to scope the Leadership Initiatives, CADA should cross-refer to, or build expressly upon, the AI Act's Article 3(1) "AI system" definition rather than coin a free-standing definition that diverges from it.
2. **Keep conduct in the AI Act.** Any obligations on how agentic AI behaves belong in the AI Act; CADA correctly focuses on infrastructure, compute and leadership Initiatives and should not be expanded to broader AI coverage.
3. **Ensure coherence.** The two instruments should be explicitly coherent, so that the concept of an "AI agent" in Union law has a single, settled meaning.

EFA supports the Union's ambition to strengthen Europe's technological capacity and resilience. We encourage the co-legislators to ensure that the final package advances that ambition through open, interoperable and risk-based measures, while preserving legal coherence and the ability of regulated European firms to manage technology risk effectively. EFA would be pleased to contribute practical input by hosting discussions with its members as the file progresses.

Yours sincerely,

Lucia Pecchini

Secretary General, on behalf of the European Fintech Association