Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Comments

Cloud and AI Development Act (CADA) 08/2026

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Florian Simon Ruhnke
Telephone: +49 30 2021-2113
E-Mail: F.Ruhnke@bvr.de

Berlin, 31. August 2026

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin
Telephone: +49 30 2021-0
https://die-dk.de/

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Comments Cloud and AI Development Act (CADA)
08/2026

I. General Remarks

The German Banking Industry Committee (GBIC) welcomes the European Commission's objective of strengthening European cloud, AI and data centre capacities and reducing strategic dependencies in key digital infrastructures. High-performing, secure and resilient digital infrastructures are essential for credit institutions' competitiveness, operational resilience, customer protection and capacity to innovate.

The proposal addresses a real challenge: Europe remains dependent on non-European providers in significant parts of the digital value chain. At the same time, digital sovereignty must not be confused with technological autarky. From the GBIC's perspective, sovereignty means strategic capability. Dependencies must be known, manageable and diversifiable; data, processes and critical functions must remain under effective control; and institutions must be able to maintain operational capability even in times of crisis.

Against this background, the GBIC particularly supports those elements of the proposal aimed at promoting competitive European offerings, research, scaling, interoperability, data centre capacity and open standards. European alternatives should succeed through performance, security, economic viability and ease of integration. They should not be imposed through direct or indirect usage requirements.

For the banking sector, it is essential that CADA be designed in a technology-open, risk-based manner and remain coherent with existing financial sector regulation. Credit institutions are already subject to DORA, which provides a comprehensive framework for ICT risk management, third-party risk management, outsourcing, concentration risks, incident management, business continuity and exit strategies. CADA must not create a second, parallel compliance layer. An explicit precedence rule in favour of the DORA framework is required.

Particularly sensitive in this regard are the provisions under Title IV on the sovereignty framework, especially Articles 29 to 31. Risk assessments, procurement requirements and any potential extension to private undertakings must remain narrowly defined, proportionate and limited to genuinely public or public-order-related use cases. Including banks within the scope of such provisions would restrict technology and provider choice, increase costs and weaken innovation without necessarily creating a corresponding or meaningful resilience benefit.

II. Supplementary Remarks of the German Banking Industry Committee

From the perspective of the German Banking Industry Committee, the following aspects should be taken into account in the further legislative process:

1. Ensure Coherence with DORA
   DORA should remain the primary framework for credit institutions with regard to ICT risks, third-party risk management, outsourcing, concentration risks and exit strategies. CADA must neither override nor duplicate existing supervisory processes. An explicit precedence rule in favour of DORA is required.

2. Maintain Coherence with Existing Financial Sector Regulation
   To avoid duplicate regulation, additional administrative burdens and resulting competitive disadvantages, the GBIC calls for the complete deletion of Article 31 ("Impact Assessments").

3. Understand Digital Sovereignty as De-Risking
   Digital sovereignty should be understood as de-risking rather than de-coupling. The objective should be the conscious management and diversification of dependencies, not the isolation of the European market or the blanket displacement of non-European providers.

4. Ensure Technology Openness and Freedom of Provider Choice
   Institutions must retain the freedom to select technologies and providers. Banks should be able to choose cloud and AI services based on performance, security, resilience, regulatory suitability and customer needs. This also includes access to high-performing international cloud, AI and model ecosystems.

5. Promote Competitive European Cloud and AI Offerings
   CADA should support the development of competitive European cloud and AI alternatives. Key success factors include investment, scalability, interoperability, portability, cybersecurity, practical usability and compatibility with existing enterprise architectures.

6. Design the Cloud Sovereignty Framework in a Risk-Based Manner
   The cloud sovereignty framework should provide transparency and reusable provider-level evidence. Sovereignty levels must not become de facto usage requirements for financial institutions.

7. Promote Open Source as an Enabler
   Open source should be promoted as an important instrument for transparency, portability and innovation. However, there should be no general open-source obligation. Critical banking applications require reliability, maintenance, liability, security patching and professional support.

III. Comments on Selected Provisions of CADA

1. Cloud and AI Leadership Initiatives and Research and Development Activities

The measures envisaged in Articles 3 to 9 to strengthen European cloud, AI and software capacities are welcome in principle. They can provide meaningful benefits if they focus not only on technological research but also on industrial usability and practical scalability.

For banks, it is essential that supported technologies become production-ready, secure, supportable, interoperable and economically viable. Research and funding programmes should therefore involve regulated user industries at an early stage and take account of requirements relating to cybersecurity, portability, auditability, regulatory compatibility and integration into existing IT architectures.

2. Union Cloud Sovereignty Framework

A common European framework for the assessment of cloud services can be beneficial for users if it improves transparency and comparability between offerings. It is particularly positive that sovereignty can be designed as a graduated concept rather than a binary distinction between “sovereign” and “non-sovereign”.

At the same time, it must be clarified that sovereignty levels are instruments for information and assurance. For financial institutions, they must not become automatic procurement requirements, licensing conditions or de facto usage obligations. What should matter is not solely the origin of a provider but whether a specific service configuration is controllable, auditable, resilient, interoperable and substitutable.

The framework should recognise existing standards, certifications and evidence where they are materially equivalent. This principle should be explicitly anchored in the Regulation. Evidence should furthermore be designed in a way that allows it to be provided at provider level and reused by multiple customers. Otherwise, there is a risk of creating an additional audit layer without delivering any meaningful risk-management benefit.

3. Third-Country Access and Technology Openness

The GBIC considers open, rules-based and non-discriminatory access for trustworthy third-country providers to be essential. The European cloud and AI market depends on innovation, competition and global connectivity. Banks in particular must retain access to high-performing global technologies as long as equivalent European alternatives are not yet available in all areas.

This applies especially to advanced AI models, foundation models and AI platforms, which are becoming increasingly important for innovation, competitiveness and the development of new use cases. Regulatory requirements should therefore not unnecessarily restrict access to high-performing international AI ecosystems, provided that appropriate governance, control and risk-management measures are in place.

The conditions for participation by providers from associated third countries should therefore be transparent, objective and predictable. Formal openness must not be undermined by requirements that are prohibitive in practice.

4. Risk Assessments and Public Procurement

Articles 29 (“Risk Assessment”) and 30 (“Public Procurement”) should remain limited to public or genuinely public-order-related use cases. Risk assessments for public authorities may be appropriate where they are based on concrete protection needs, data sensitivity, operational criticality and realistic threat scenarios.

The classification of an activity as critical or essential under the NIS2 Directive must not automatically lead to its being regarded as contributing to the maintenance of public order within the meaning of Article 29. Otherwise, regulated financial services would also fall within scope, even though they do not constitute core governmental functions.

Banking services are economically important and, in some cases, systemically relevant. Nevertheless, they are not comparable to core state functions such as defence, law enforcement, public security or the administration of justice and should therefore not be treated as public-order functions. Public procurement requirements must also not indirectly spill over into financial institutions, particularly where recognised alternatives are unavailable, technically unsuitable or economically disproportionate.

5. Coherence with Existing Financial Sector Regulation

Article 31 is the most critical provision for the banking sector. The possibility of imposing additional impact assessments and risk-mitigation measures on private undertakings operating in highly critical sectors risks creating a parallel compliance regime alongside DORA. Therefore, Article 31 should be deleted in its entirety.

Credit institutions are already subject to a comprehensive and directly applicable framework for digital operational resilience under DORA. The Regulation includes requirements relating to ICT risk management, third-party risk management, outsourcing, concentration risks, incident management, business continuity and exit strategies. Additional CADA-related risk analyses or usage expectations would create duplicate regulation, legal uncertainty and unnecessary administrative burden without providing a corresponding resilience benefit. An extension to financial institutions would therefore not be proportionate.

6. Union Added Value Criteria, Joint Procurement and EuroCloud Federation

Criteria for European added value can support innovation and resilience if they focus on security of supply, interoperability, open standards, cybersecurity and scalability. Pure origin-based criteria, by contrast, risk creating protectionist effects and may reduce the quality and availability of suitable services.

Joint procurement and a EuroCloud Federation can be beneficial for the public sector provided they remain voluntary, transparent and competitive. However, they must not become a reference model for private-sector obligations and must not create direct or indirect usage expectations for banks.

7. Open Source

The GBIC welcomes the promotion of open digital ecosystems. Open source can increase transparency, verifiability, portability and innovation and can reduce lock-in risks. Nevertheless, open source is not automatically secure, sovereign or suitable for every critical use case.

Particularly in the banking sector, robust security processes, long-term maintenance, rapid vulnerability remediation, clear responsibilities, liability, service levels and professional support are essential. CADA should therefore promote open source but not mandate it. The decisive factor is a risk-based approach that ensures security and operational resilience. CADA should therefore serve merely as an enabler for open source.

IV. Concluding Remarks

CADA can make an important contribution to strengthening European digital sovereignty if it is designed as an enabling industrial and regulatory framework. The GBIC supports the development of competitive European cloud, AI and data centre capacities, greater provider diversity and improved transparency regarding the sovereignty characteristics of digital services.

However, it is essential that digital sovereignty is not translated into market isolation, usage obligations or duplicate regulation. For banks, technology openness, freedom of provider choice and coherence with DORA must be preserved. European alternatives should succeed through quality, security, performance and economic viability, not through direct or indirect mandates.

The GBIC will continue to engage constructively in the legislative process and advocates a framework that strengthens digital resilience and strategic capability without undermining competitiveness, innovation and workable financial-sector regulation.