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

# Stellungnahme

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

*Lobbyregister-Nr. R001459*
*EU-Transparenzregister-Nr. 52646912360-95*

Berlin, 31. August 2026

Federführer:
Bundesverband der Deutschen
Volksbanken und Raiffeisenbanken e.V.
Schellingstraße 4 | 10785 Berlin
Telefon: +49 30 2021-0
Telefax: +49 30 2021-1900
https://die-dk.de/

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

**Stellungnahme** Cloud and AI Development Act (CADA)
08/2026

## I. Allgemeine Anmerkungen

Die Deutsche Kreditwirtschaft (DK) begrüßt das Ziel der Europäischen Kommission, die europäischen Cloud-, KI- und Rechenzentrumskapazitäten zu stärken und strategische Abhängigkeiten in zentralen digitalen Infrastrukturen zu verringern. Leistungsfähige, sichere und resiliente digitale Infrastrukturen sind für Kreditinstitute eine wesentliche Voraussetzung für Wettbewerbsfähigkeit, operationelle Resilienz, Kundenschutz und Innovationsfähigkeit.

Der Vorschlag adressiert damit ein reales Problem: Europa ist in wesentlichen Teilen der digitalen Wertschöpfungskette auf außereuropäische Anbieter angewiesen. Zugleich darf digitale Souveränität nicht mit technologischer Autarkie verwechselt werden. Souveränität bedeutet aus Sicht der DK strategische Handlungsfähigkeit: Abhängigkeiten müssen bekannt, steuerbar und diversifizierbar sein; Daten, Prozesse und kritische Funktionen müssen wirksam kontrolliert werden können; und Institute müssen auch in Krisensituationen handlungsfähig bleiben.

Vor diesem Hintergrund unterstützt die DK insbesondere die Elemente des Vorschlags, die auf den Aufbau wettbewerbsfähiger europäischer Angebote, Forschung, Skalierung, Interoperabilität, Rechenzentrumskapazitäten und offene Standards gerichtet sind. Europäische Alternativen müssen durch Leistungsfähigkeit, Sicherheit, Wirtschaftlichkeit und Integrationsfähigkeit überzeugen. Sie sollten nicht durch direkte oder indirekte Nutzungspflichten erzwungen werden.

Für den Bankensektor ist entscheidend, dass CADA technologieoffen, risikobasiert und kohärent mit bestehenden Finanzmarktregelungen ausgestaltet wird. Kreditinstitute unterliegen mit DORA bereits einem umfassenden Rechtsrahmen für IKT-Risikomanagement, Drittparteiensteuerung, Auslagerungen, Konzentrationsrisiken, Vorfallmanagement, Geschäftsfortführung und Exit-Strategien. CADA darf daneben keine zweite, parallele Compliance-Ebene schaffen. Erforderlich ist eine ausdrückliche Vorrangregelung zugunsten des DORA-Rahmens.

Besonders sensibel sind in diesem Zusammenhang die Regelungen des Titels IV zum Souveränitätsrahmen, insbesondere die Artikel 29 bis 31. Risikobewertungen, Beschaffungsvorgaben und eine mögliche Ausweitung auf private Unternehmen müssen eng begrenzt, verhältnismäßig und auf tatsächlich öffentliche beziehungsweise ordnungsrelevante Anwendungsfälle zugeschnitten bleiben. Eine Erfassung von Banken würde Technologie- und Anbieterwahl einschränken, zusätzliche Kosten verursachen und Innovationsfähigkeit schwächen, ohne zwingend einen entsprechenden oder wesentlichen Resilienzgewinn zu bewirken.

## II. Ergänzende Anmerkungen der Deutschen Kreditwirtschaft

Aus Sicht der Deutschen Kreditwirtschaft sind im weiteren Gesetzgebungsverfahren insbesondere die folgenden Aspekte zu berücksichtigen:

1. Kohärenz mit DORA sicherstellen
   DORA sollte für Kreditinstitute der maßgebliche Rahmen für IKT-Risiken, Drittparteiensteuerung, Auslagerungen, Konzentrationsrisiken und Exit-Strategien bleiben. CADA darf bestehende finanzaufsichtliche Prozesse weder überlagern noch duplizieren. Erforderlich ist eine ausdrückliche Vorrangregelung zugunsten des DORA-Rahmens.

2. Kohärenz mit bestehenden Finanzmarktregelungen wahren
   Um Doppelregulierung, zusätzlichen bürokratischen Aufwand und daraus resultierende Wettbewerbsnachteile zu vermeiden, fordert die DK die vollständige Streichung von Artikel 31 („Impact Assessments“).

3. Digitale Souveränität als De-Risking verstehen
   Digitale Souveränität sollte als De-Risking und nicht als De-Coupling verstanden werden. Ziel sollte die bewusste Steuerung und Diversifizierung von Abhängigkeiten sein, nicht die Abschottung des europäischen Marktes oder die pauschale Verdrängung außereuropäischer Anbieter.

4. Technologieoffenheit und Anbieterwahlfreiheit sicherstellen
   Die Technologie- und Anbieterwahlfreiheit der Institute sollte gewahrt bleiben. Banken müssen Cloud- und KI-Dienste nach Leistungsfähigkeit, Sicherheit, Resilienz, regulatorischer Eignung und Kundenbedarf auswählen können. Dies umfasst auch den Zugang zu leistungsfähigen internationalen Cloud-, KI- und Modellökosystemen.

5. Aufbau wettbewerbsfähiger europäischer Cloud- und KI-Angebote fördern
   CADA sollte den Aufbau leistungsfähiger europäischer Cloud- und KI-Alternativen unterstützen. Entscheidend sind Investitionen, Skalierung, Interoperabilität, Portabilität, Cybersicherheit, Praxistauglichkeit und Anschlussfähigkeit an bestehende Unternehmensarchitekturen.

6. Cloudsouveränitätsrahmen risikobasiert ausgestalten
   Der Cloudsouveränitätsrahmen sollte Transparenz und wiederverwendbare Nachweise auf Anbieterebene schaffen. Souveränitätslevel dürfen jedoch nicht zu faktischen Nutzungsvorgaben für Finanzinstitute werden.

7. Open Source als Enabler fördern
   Open Source sollte als wichtiges Instrument für Transparenz, Portabilität und Innovationsfähigkeit gefördert werden. Es sollte jedoch keine pauschale Open-Source-Pflicht geben; kritische Bankanwendungen benötigen Verlässlichkeit, Wartung, Haftung, Sicherheitspatches und professionellen Support.

## III. Anmerkungen zu ausgewählten Bestimmungen des CADA

### 1. Cloud- und KI-Leitinitiativen sowie Forschungs- und Entwicklungsaktivitäten

Die in den Artikeln 3 bis 9 vorgesehenen Maßnahmen zur Stärkung europäischer Cloud-, KI- und Softwarekapazitäten sind grundsätzlich zu begrüßen. Sie können einen Beitrag leisten, wenn sie nicht nur technologische Forschung, sondern auch industrielle Nutzbarkeit und praktische Skalierung in den Mittelpunkt stellen.

Für Banken ist entscheidend, dass geförderte Technologien produktionsreif, sicher, supportfähig, interoperabel und wirtschaftlich tragfähig sind. Forschungs- und Förderprogramme sollten daher frühzeitig regulierte Anwenderbranchen einbeziehen und Anforderungen an Cybersicherheit, Portabilität, Auditierbarkeit, regulatorische Kompatibilität und Integration in bestehende IT-Architekturen berücksichtigen.

### 2. Unionsrahmen für Cloudsouveränität

Ein gemeinsamer europäischer Rahmen zur Bewertung von Clouddiensten kann für Nutzer hilfreich sein, wenn er Transparenz schafft und die Vergleichbarkeit von Angeboten verbessert. Positiv ist insbesondere, dass Souveränität als graduelles Konzept ausgestaltet werden kann und nicht binär als 'souverän' oder 'nicht souverän' verstanden werden muss.

Gleichzeitig muss klargestellt werden, dass Souveränitätslevel Informations- und Absicherungsinstrumente sind. Sie dürfen für Finanzinstitute nicht zu automatischen Beschaffungsvorgaben, Zulassungsvoraussetzungen oder faktischen Nutzungspflichten werden. Entscheidend sollte nicht allein die Herkunft eines Anbieters sein, sondern ob eine konkrete Dienstekonfiguration steuerbar, auditierbar, resilient, interoperabel und substituierbar ist.

Der Rahmen sollte bestehende Standards, Zertifizierungen und Nachweise anerkennen, soweit sie sachlich gleichwertig sind. Dies sollte verbindlich im Verordnungstext verankert werden. Nachweise sollten zudem so ausgestaltet werden, dass sie auf Anbieterebene erbracht und von mehreren Nutzern wiederverwendet werden können. Andernfalls droht eine zusätzliche Auditschicht ohne echten Risikonutzen.

## 3. Drittstaatenzugang und Technologieoffenheit

Die DK hält einen offenen, regelbasierten und diskriminierungsfreien Zugang vertrauenswürdiger Drittstaatenanbieter für erforderlich. Der europäische Cloud- und KI-Markt ist auf Innovation, Wettbewerb und internationale Anschlussfähigkeit angewiesen. Gerade Banken müssen Zugang zu leistungsfähigen globalen Technologien behalten, solange europäische Alternativen noch nicht in allen Bereichen gleichwertig verfügbar sind.

Dies gilt insbesondere für leistungsfähige KI-Modelle, Foundation Models und KI-Plattformen, die für Innovation, Wettbewerbsfähigkeit und die Entwicklung neuer Anwendungsfälle zunehmend von Bedeutung sind. Regulatorische Anforderungen sollten daher den Zugang zu leistungsfähigen internationalen KI-Ökosystemen nicht unnötig einschränken, sofern angemessene Governance-, Kontroll- und Risikomanagementmaßnahmen gewährleistet sind.

Die Voraussetzungen für die Beteiligung von Anbietern aus assoziierten Drittstaaten sollten daher transparent, objektiv und vorhersehbar sein. Formale Offenheit darf nicht durch faktisch prohibitive Anforderungen unterlaufen werden.

## 4. Risikobewertungen und öffentliche Beschaffung

Die Artikel 29 („Risk Assessment“) und 30 („Public Procurement“) sollten eng auf öffentliche beziehungsweise tatsächlich ordnungsrelevante Anwendungsfälle begrenzt bleiben. Eine Risikobewertung für öffentliche Stellen kann sinnvoll sein, wenn sie auf konkrete Schutzbedarfe, Datensensibilität, operative Kritikalität und realistische Bedrohungsszenarien abstellt.

Die Einstufung einer Tätigkeit als kritisch oder wesentlich nach der NIS2-Richtlinie darf nicht automatisch zu einer Einordnung als Beitrag zur Aufrechterhaltung der öffentlichen Ordnung im Sinne des Artikels 29 führen. Andernfalls würden auch regulierte Finanzdienstleistungen erfasst, obwohl sie nicht den Charakter staatlicher Kernfunktionen aufweisen.

Bankdienstleistungen sind zwar wirtschaftlich bedeutsam und in einzelnen Fällen systemrelevant, stehen jedoch nicht auf einer Ebene mit staatlichen Kernfunktionen wie Verteidigung, Strafverfolgung, öffentlicher Sicherheit oder Rechtspflege und sollten daher nicht als öffentliche Ordnungsfunktionen behandelt werden. Auch Beschaffungsvorgaben für den öffentlichen Sektor dürfen nicht indirekt auf Finanzinstitute ausstrahlen, insbesondere wenn anerkannte Alternativen nicht verfügbar, technisch ungeeignet oder wirtschaftlich unverhältnismäßig sind.

## 5. Kohärenz mit bestehenden Finanzmarktregelungen

Artikel 31 stellt aus Sicht der DK die für den Bankensektor kritischste Bestimmung dar. Die Möglichkeit, privaten Unternehmen in hochkritischen Sektoren zusätzliche Folgenabschätzungen und Risikominderungsmaßnahmen aufzuerlegen, droht, ein zu DORA paralleles Compliance-Regime zu produzieren. Daher sollte Artikel 31 aus Sicht der DK vollständig gestrichen werden.

Mit DORA besteht für Kreditinstitute bereits ein umfassender und unmittelbar anwendbarer Rahmen für digitale operationelle Resilienz. Die Verordnung enthält Anforderungen an IKT-Risikomanagement, Drittparteiensteuerung, Auslagerungen, Konzentrationsrisiken, Vorfallmanagement, Business Continuity und Exit-Strategien. Zusätzliche CADA-bezogene Risikoanalysen oder Nutzungserwartungen würden Doppelregulierung, Rechtsunsicherheit und zusätzlichen bürokratischen Aufwand verursachen, ohne einen entsprechenden Mehrwert für die Resilienz zu schaffen. Eine Ausweitung auf Finanzinstitute wäre daher nicht verhältnismäßig.

## 6. Kriterien für Unionsmehrwert, gemeinsame Beschaffung und EuroCloud Federation

Kriterien für einen europäischen Mehrwert können Innovation und Resilienz unterstützen, wenn sie auf Versorgungssicherheit, Interoperabilität, offene Standards, Cybersicherheit und Skalierbarkeit ausgerichtet

sind. Reine Herkunftskriterien bergen dagegen das Risiko protektionistischer Effekte und können die Qualität und Verfügbarkeit geeigneter Dienste beeinträchtigen.

Gemeinsame Beschaffung und eine EuroCloud Federation können für den öffentlichen Sektor sinnvoll sein, sofern sie freiwillig, transparent und wettbewerblich ausgestaltet werden. Sie dürfen jedoch nicht zum Referenzmodell für private Pflichten werden und keine direkten oder indirekten Nutzungserwartungen für Banken begründen.

### 7. Open Source

Die DK begrüßt die Förderung offener digitaler Ökosysteme. Open Source kann Transparenz, Prüfbarkeit, Portabilität und Innovationsfähigkeit stärken und Lock-in-Risiken reduzieren. Gleichwohl ist Open Source nicht automatisch sicher, souverän oder für jeden kritischen Einsatz geeignet.

Gerade im Bankensektor kommt es auf belastbare Sicherheitsprozesse, langfristige Wartung, schnelle Schwachstellenbehebung, klare Verantwortlichkeiten, Haftung, Service Levels und professionellen Support an. CADA sollte Open Source daher fördern, aber nicht verordnen. Entscheidend ist ein risikobasierter Einsatz, der Sicherheit und operationelle Resilienz gewährleistet. CADA sollte für Open Source also lediglich ein Enabler sein.

## IV. Schlussbemerkungen

CADA kann einen wichtigen Beitrag zur Stärkung der europäischen digitalen Souveränität leisten, wenn der Vorschlag als befähigender Industrie- und Ordnungsrahmen ausgestaltet wird. Die DK unterstützt den Aufbau wettbewerbsfähiger europäischer Cloud-, KI- und Rechenzentrumskapazitäten, mehr Anbieterdiversität und bessere Transparenz über Souveränitätsmerkmale von Diensten.

Entscheidend ist jedoch, dass digitale Souveränität nicht in Abschottung, Nutzungspflichten oder Doppelregulierung übersetzt wird. Für Banken müssen Technologieoffenheit, Anbieterwahlfreiheit und DORA-Kohärenz gewahrt bleiben. Europäische Alternativen sollten durch Qualität, Sicherheit, Leistung und Wirtschaftlichkeit überzeugen, nicht durch direkten oder indirekten Zwang.

Die DK wird den weiteren Gesetzgebungsprozess konstruktiv begleiten und setzt sich für eine Ausgestaltung ein, die digitale Resilienz und strategische Handlungsfähigkeit stärkt, ohne Wettbewerbsfähigkeit, Innovation und praxistaugliche Finanzmarktregulierung zu beeinträchtigen.