Positionspapier

Das Tech Sovereignty Package – eine Perspektive aus der Finanzindustrie

Risikobasiertes Management digitaler Abhängigkeiten als Grundlage für die europäische Souveränität

Juli 2026

1. Executive Summary

Das Tech Sovereignty Package ist in seiner aktuellen Entwurfsfassung ein wichtiger Meilenstein auf dem Weg zu größerer europäischer Souveränität, der auch von der Finanzwirtschaft grundsätzlich unterstützt wird. Es erweitert bestehende, primär risikobasierte Regulierungsansätze – darunter DORA und NIS2 – um zusätzliche Dimensionen wie Eigentum, Kontrolle, Einfluss von Drittstaaten sowie Anforderungen an Software- und Lieferketten, insbesondere im Kontext der öffentlichen Beschaffung.

Primärer Adressat des Cloud & AI Development Act (CADA) ist der öffentliche Sektor. Über die Ausgestaltung von Assurance Levels, Beschaffungskriterien und Zulassungslogiken wird der Rahmen jedoch unmittelbare Auswirkungen auf die Struktur des europäischen Cloud- und KI-Ökosystems haben. Eine zentrale Gestaltungsfrage ist, auf welcher Ebene regulatorische Anforderungen ansetzen sollten. Ein stärkeres, konsistentes und risikobasiertes Anforderungsset für Cloud- und Rechenzentrumsanbieter kann dazu beitragen, nachgelagerte Nutzer – etwa Banken, Sparkassen und öffentliche Einrichtungen – von redundanten Prüf-, Nachweis- und Kontrollaufwänden zu entlasten. Voraussetzung dafür ist eine kohärente Ausgestaltung von Assurance Levels und Verifikationssystemen, die Skaleneffekte auf Anbieterseite ermöglicht und Doppelregulierung auf Nutzerseite vermeidet.

Diese Markt- und Infrastrukturlogik bildet zugleich die technische Grundlage hoch digitalisierter kritischer Sektoren – insbesondere von Banken und Finanzmarktinfrastrukturen, die in hohem Maße von denselben Cloud-, Plattform- und KI-Diensten abhängig sind.

Diese Abhängigkeit tritt im Bereich der künstlichen Intelligenz noch deutlicher zutage. KI-Systeme sind zunehmend nicht nur modellbasierte Anwendungen, sondern hängen vom gesamten Cloud- und KI-Stack ab, einschließlich Recheninfrastruktur, Modellzugang, MLOps, Orchestrierungsschichten, Retrieval-Systemen, Logging, Monitoring, Telemetrie und Supportstrukturen. Souveränitätsanforderungen im Rahmen von CADA sollten KI-Dienste daher nicht isoliert bewerten, sondern die gesamte operative Konfiguration sowie die Fähigkeit der Nutzer berücksichtigen, Datenflüsse zu kontrollieren, angemessene Data

Bundesverband Öffentlicher Banken Deutschlands, VÖB, e.V.
Lennéstraße 11, 10785 Berlin
www.voeb.de

Präsident: Thomas Groß
Stellvertretender Präsident: Erk Westermann-Lammers
Hauptgeschäftsführerin und geschäftsführendes Vorstandsmitglied: Iris Bethge-Krauß

Registernummer im Lobbyregister: R001169

Governance sicherzustellen, Abhängigkeiten zu auditieren und realistische Exit- und Substitutionsoptionen aufrechtzuerhalten.
Vor diesem Hintergrund ist CADA nicht nur ein Beschaffungs- oder Verwaltungsrahmen, sondern ein strukturbildender Eingriff in die digitale Wertschöpfungs- und Lieferkettenarchitektur mit sektorübergreifenden Wirkungen. Es ist daher sachgerecht, die unter DORA entwickelten Governance-, Risiko- und Kontrollmechanismen als praxisnahen Referenzrahmen in die weitere Ausgestaltung einzubeziehen.
DORA zeigt, wie komplexe, globale IKT-Abhängigkeiten risikobasiert gesteuert werden können, ohne die operative Steuerbarkeit und Innovationsfähigkeit durch strukturelle Marktsegmentierung, pauschale Anbieterklassifizierungen oder eigentumsbezogene Ausschlüsse zu beeinträchtigen.
Daraus lassen sich vier zentrale Prinzipien ableiten:

- **Steuerungsfähigkeit statt struktureller Marktsegmentierung**
- **Datensouveränität als funktionaler Anker von Souveränität**
- **Risikobasierte Anwendung statt pauschaler Klassifizierung**
- **Interoperabilität und Portabilität als Ermöglicher von Exit-Fähigkeit und geringeren Lock-in-Risiken**

Für den öffentlichen Sektor ergibt sich daraus die Chance, auf bereits etablierte und praktisch erprobte Governance-Logiken zurückzugreifen – insbesondere bei der Definition von Assurance Levels, Nachweisanforderungen und Beschaffungskriterien. Dies ist auch mit Blick auf die zunehmende Komplexität öffentlicher Beschaffungsprozesse relevant, da zusätzliche Souveränitätsanforderungen andernfalls zu längeren Beschaffungszyklen, höheren Umsetzungsaufwänden und möglichen Einschränkungen der Anbietervielfalt führen könnten.
Aus Sicht der Finanzwirtschaft besteht zudem ein eigenständiges Interesse an einer verhältnismäßigen und risikobasierten Ausgestaltung von CADA. Banken nutzen dieselben digitalen Infrastrukturen wie der öffentliche Sektor und unterliegen zugleich strengen Anforderungen an Resilienz und Auslagerungen, einschließlich DORA. Die konkrete Ausgestaltung von CADA ist daher ein relevanter Faktor für ihre operative Handlungsfähigkeit, Kostenstruktur und Innovationsfähigkeit.
Vor diesem Hintergrund ist die Finanzwirtschaft nicht nur mittelbar betroffen, sondern systemischer Nutzer der zugrunde liegenden Cloud- und KI-Infrastruktur. Die folgenden Positionen sind daher als Beitrag aus der praktischen Umsetzungserfahrung bei der Steuerung komplexer IKT-Abhängigkeiten und hoch regulierter digitaler Ökosysteme zu verstehen. Sie sollen eine kohärente, interoperable und verhältnismäßige Weiterentwicklung des europäischen Souveränitätsrahmens unterstützen – im Einklang mit etablierten Regulierungslogiken unter DORA und NIS2.

2. Kernpositionen

Aus Sicht der Banken lässt sich digitale Souveränität wie folgt definieren:

> **Digitale Souveränität** ist die Fähigkeit eines Finanzinstituts, über alle Ebenen der IKT-Wertschöpfungskette hinweg eigenständig und autonom Entscheidungen bei der Auswahl leistungsfähiger und vertrauenswürdiger Vertragspartner zu treffen, diese verantwortungsvoll zu nutzen und sie bei Bedarf weiterzuentwickeln oder zu substituieren. Ziel ist es, sicherzustellen, dass die für Geschäftsprozesse erforderlichen IKT-Dienste gegenüber externen

Einflüssen – etwa geopolitischen Störungen – resilient bleiben und sicher, integer sowie verfügbar sind.

Digitale Souveränität bedeutet nicht Autonomie oder die ausschließliche Nutzung von Lösungen und Produkten aus der EU. Vielmehr geht es um Entscheidungssouveränität über Daten, Infrastruktur und Anwendungen – einschließlich der Nutzung globaler Anbieter –, sofern eine selbstbestimmte und sichere Nutzung gewährleistet ist und Lock-in-Szenarien vermieden werden. Hybrid- und Multi-Cloud-Strategien sowie moderne Architekturen erhöhen Resilienz und Flexibilität und bieten daher erhebliche Chancen. Sie sind jedoch typischerweise mit erheblicher zusätzlicher Komplexität und nicht zuletzt mit Kosten verbunden. Der Einsatz neuer Technologien wie KI erfordert transparente Governance, eine strategische Risikobewertung und ein aktives Management von Abhängigkeiten.
Im Kontext von KI erfordert digitale Souveränität zudem Steuerbarkeit auf der Modell-, Plattform- und Orchestrierungsebene. Dazu gehören Transparenz darüber, wo Training, Inferenz, Logging, Monitoring, Telemetrie und Support stattfinden, ob Prompts, Embeddings, Outputs, Metadaten oder Nutzungsdaten für Training, Fine-Tuning oder Serviceverbesserung verwendet werden dürfen und ob der Nutzer technisch und vertraglich Modelle, Anbieter oder Deployment-Umgebungen ohne unverhältnismäßige operative Störungen wechseln kann.

Position 1 – Steuerungsfähigkeit hat Vorrang vor Autonomie
Die unter CADA vorgesehenen Assurance Levels dürfen nicht primär zu einer Marktsegmentierung nach Eigentum oder Herkunft führen. Andernfalls besteht insbesondere auf höheren Stufen – vor allem bei Level 3 und 4 – das Risiko, dass faktisch nur EU-kontrollierte Anbieter in Betracht kommen, während globale Hyperscaler – einschließlich US-amerikanischer Cloud-Anbieter – selbst dann ausgeschlossen würden, wenn eine nachweislich kontrollierte und regelkonforme Nutzung vorliegt.
Aus Sicht der Bankpraxis und der Erfahrungen mit DORA sollte daher folgender Grundsatz gelten:

Position 1
Wir fordern, dass nicht allein die Herkunft des Anbieters maßgeblich ist, sondern die nachweisbare Steuerbarkeit, Auditierbarkeit, Interoperabilität und Exit-Fähigkeit der konkreten Nutzungskonfiguration.

Dadurch könnte CADA stärker an bestehende risikobasierte Logiken anknüpfen, statt diese durch strukturelle Ausschlusskriterien zu überlagern.

Position 2 – Datensouveränität als kompatibler, zentraler Anker von Souveränität
Die im Tech Sovereignty Package adressierte digitale Souveränität sollte Datensouveränität als zentrale, aber nicht hinreichende Dimension verstehen.
Die Erfahrungen des Bankensektors unter DORA zeigen, dass Datenkontrolle auch in globalen Cloud-Umgebungen technisch durchgesetzt werden kann, etwa durch kundenseitige Schlüsselinhaberschaft, Ende-zu-Ende-Verschlüsselung und granulare Zugriffskonzepte.

Im Kontext von CADA ist daher entscheidend:

> **Position 2**
> Wir fordern, Datensouveränität als gleichwertiges Kriterium neben strukturellen Kontroll- und Eigentumsaspekten anzuerkennen und sie in der praktischen Anwendung von Cloud- und KI-Diensten als funktionalen Nachweis digitaler Souveränität zu berücksichtigen.

Dies ist insbesondere deshalb relevant, weil extraterritoriale Rechtsregime – etwa Zugriffsmechanismen aus Drittstaaten – unabhängig vom Speicherort der Daten gelten können.

Position 3 – Risikobasierte Anwendung von Assurance Levels statt pauschaler Klassifizierung
Die Erfahrungen aus DORA zeigen deutlich, dass Kritikalität kontextabhängig ist – etwa im Hinblick auf Workload, System oder Geschäftsprozess – und dass selbst dieselbe Technologie unterschiedliche Risikoprofile aufweisen kann. Auf CADA übertragen bedeutet dies, dass nicht jede öffentliche IT-Anwendung Level 3 oder 4 erfordert und insbesondere nicht jeder Cloud- oder KI-Anwendungsfall im öffentlichen Sektor dies rechtfertigt.

> **Position 3**
> Wir fordern, dass die Einführung von Assurance Levels unter CADA nicht zu einer pauschalen Zuordnung von Technologien oder Anbietern führt, sondern auf Grundlage der spezifischen Anforderungen des jeweiligen Anwendungsfalls risikobasiert erfolgt.

Position 4 – Rolle der Risikobewertung nach Artikel 29 als Systemfilter
Die Risikobewertung nach Artikel 29 durch die Mitgliedstaaten führt eine entscheidende vorgelagerte Klassifizierungsebene ein, die bestimmt, ob Tätigkeiten des öffentlichen Sektors als relevant für die Aufrechterhaltung der öffentlichen Ordnung gelten. Diese Bewertung beeinflusst unmittelbar die Zuordnung von Assurance Levels nach Artikel 30 und wirkt damit als struktureller Gatekeeper zwischen politischer Zielsetzung und operativen Beschaffungsergebnissen. Unterschiede in der nationalen Risikoauslegung können sich folglich erheblich auf die praktische Anwendung der Assurance Levels in den Mitgliedstaaten auswirken.

> **Position 4**
> Wir fordern, dass Banken und Förderbanken nicht pauschal als Beitragende zur Aufrechterhaltung der öffentlichen Ordnung im Sinne von Artikel 29 CADA eingestuft werden. Ihre regulären Tätigkeiten 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.

Eine Einbeziehung sollte daher auf einer klar begründeten, tätigkeitsbezogenen und risikobasierten Bewertung beruhen und nicht auf sektorweiten Annahmen. Auch wenn Zahlungs- und Bargelddienstleistungen in Krisensituationen an Bedeutung gewinnen können, sind wir der Auffassung,

dass solche Ausnahmesituationen nicht die allgemeine Einordnung von Banken nach Artikel 29 CADA bestimmen sollten.
Eine weite Auslegung würde erhebliche rechtliche und operative Unsicherheit schaffen, da unklar bliebe, unter welchen Voraussetzungen Institute in den Anwendungsbereich der Bewertung nach Artikel 29 und der daraus folgenden Anforderungen an Assurance Levels und Beschaffung fallen.
Vor diesem Hintergrund sollte die potenzielle Ausweitung von Souveränitätsanforderungen auf den Privatsektor nach Artikel 31 entweder substanziell präzisiert, spezifiziert und im Umfang begrenzt oder bis zur Etablierung eines klaren, verhältnismäßigen und risikobasierten Anwendungsrahmens gestrichen werden. Eine Ausdehnung von Verpflichtungen, die an Bewertungen der öffentlichen Ordnung anknüpfen, auf privatwirtschaftliche Akteure ohne hinreichende Rechtssicherheit würde die Compliance-Kosten erhöhen und das Risiko uneinheitlicher Anwendung in den Mitgliedstaaten verstärken.

Position 5 – Open Source als Governance-Instrument, nicht als Definition von Souveränität
Im Kontext von CADA ist Open Source kein Souveränitätsziel an sich, sondern ein mögliches Mittel zur Stärkung von Transparenz, Portabilität und Auditierbarkeit.
Die Erfahrungen aus dem Bankensektor zeigen jedoch, dass Open Source Abhängigkeiten nicht automatisch reduziert oder Transparenz erhöht. Vielmehr verlagert sich Verantwortung auf den Nutzer, einschließlich laufender Weiterentwicklung, Betrieb und Sicherheitsmanagement sowie der Gefahr technischer Schulden durch vernachlässigte Updates. Dadurch entstehen häufig neue Abhängigkeiten auf der operativen Ebene sowie bei Integration und Lieferketten. Dies ist besonders relevant für KI- und Plattformdienste, bei denen Governance weiterhin entscheidend bleibt.
CADA sollte Open Source daher als Enabler behandeln, nicht als regulatorische Präferenz.

> **Position 5**
> Wir fordern, Open Source differenziert zu bewerten, ohne Open Source als solchem eine ausschlaggebende Rolle für Souveränität zuzuschreiben.

Position 6 – KI-getriebene Abhängigkeiten müssen transparent und realistisch gesteuert werden
Im Bereich der künstlichen Intelligenz entstehen derzeit strukturelle und kurzfristig oft unvermeidbare Marktabhängigkeiten von einer kleinen Zahl globaler Anbieter, insbesondere bei Foundation Models, cloudbasierten KI-Diensten und KI-Plattformökosystemen.
Insbesondere Prompts, Embeddings, Modellausgaben, Tool Calls, Logs, Metadaten und Nutzungsdaten können sensible geschäftliche, kundenbezogene, sicherheitsrelevante oder regulatorische Informationen enthalten und sollten daher als potenziell sensible Daten behandelt werden.
Eine strikte Anwendung hoher Assurance Levels könnte dazu führen, dass öffentliche Stellen und mittelbar auch regulierte Sektoren von zentralen technologischen Innovationspfaden abgeschnitten werden. Zugleich darf die Nutzung externer KI-Dienste nicht zu unkontrollierten Datenflüssen, verborgenem Training oder Fine-Tuning durch Anbieter, intransparenten Modelländerungen oder faktischer Nicht-Portabilität KI-basierter Prozesse führen. Dies ist besonders relevant für aufkommende agentische KI-Systeme, die mit Tools interagieren, auf Datenquellen zugreifen und operative Handlungen auslösen können. In solchen Fällen sollten Souveränitätsanforderungen angemessene

Governance-Sicherungen gewährleisten, einschließlich menschlicher Aufsicht, Auditierbarkeit, Handlungsgrenzen, Incident Management sowie wirksamer Abschalt- und Substitutionsmechanismen.

Position 6
Wir fordern, Souveränitätsanforderungen im Bereich KI so auszugestalten, dass die risikobasierte Nutzung externer KI-Dienste weiterhin möglich bleibt, ohne den Zugang zu leistungsfähigen KI-Modellen und Innovationsökosystemen unnötig einzuschränken, sofern angemessene Governance- und Kontrollmechanismen, Transparenz hinsichtlich Datennutzung und Modellbetrieb sowie realistische Exit- und Substitutionspfade über den gesamten KI-Stack hinweg bestehen.

In diesem Zusammenhang verstärken eingeschränkte Interoperabilität und Portabilität in KI-Ökosystemen die strukturelle Abhängigkeit von einer kleinen Zahl von Anbietern zusätzlich, wodurch wirksame Substitutions- und Exit-Strategien in der Praxis erschwert werden.

Position 7 – Wirtschaftliche Risiken müssen berücksichtigt und „Pseudo-Souveränität“ vermieden werden
Auch die Kostenentwicklung stellt ein strategisches Souveränitätsrisiko dar, wenn geopolitisch bedingte Preissteigerungen, Handelsbeschränkungen oder Zölle den Zugang zu Diensten faktisch einschränken und damit Wirkungen erzeugen, die einem Export- oder Nutzungsverbot ähneln.
Ein zentrales Risiko von CADA liegt darüber hinaus im Entstehen von Pseudo-Souveränität: Formale Kriterien – etwa EU-Eigentum oder EU-Gerichtsbarkeit – sind erfüllt, während tatsächliche Abhängigkeiten in Software, Hardware oder betrieblicher Infrastruktur fortbestehen.
Gleichzeitig besteht das Risiko von Sekundäreffekten wie der Verlagerung von Abhängigkeiten auf Systemintegratoren, Offshore-Betriebsmodelle oder „EU-gebrandete“ Infrastrukturen mit globalen Kernabhängigkeiten.
Dieses Risiko ist besonders relevant für KI-Dienste, die als „souverän“, „privat“, „vertrauenswürdig“ oder „sicher“ vermarktet werden. Solche Aussagen sollten nicht allein anhand von Eigentum, Gerichtsbarkeit, Branding oder Deployment-Standort bewertet werden. Maßgeblich ist vielmehr die effektive Steuerbarkeit und Auditierbarkeit des zugrunde liegenden KI-Stacks, einschließlich Modelle, Plattformen, Control Planes, Datenverarbeitung, Telemetrie, Supportstrukturen, Unterauftragnehmern und Software-Lieferketten.

Position 7
Wir fordern, die Bewertung von Souveränität konsequent an der gesamten Wertschöpfungs- und Lieferkette auszurichten und nicht allein an formalen Unternehmensstrukturen.

3. Erwartungen an die Politik

Wir erwarten von den politischen Entscheidungsträgern, bei der Weiterentwicklung des Tech Sovereignty Package die Erfahrungen aus bestehenden Regulierungsrahmen wie DORA und NIS2

systematisch zu berücksichtigen und eine konsistente regulatorische Kohärenz zwischen sektorübergreifenden und sektorspezifischen Anforderungen sicherzustellen.
Darüber hinaus sollte digitale Souveränität als strategisches Ziel konsequent mit Innovationsfähigkeit, Wettbewerbsfähigkeit und operativer Resilienz in Einklang gebracht werden; entstehende Zielkonflikte sollten transparent und nachvollziehbar bewertet werden.
Schließlich erwarten wir, dass die praktische Umsetzbarkeit neuer Souveränitätsanforderungen frühzeitig geprüft wird und betroffene Nutzerbranchen – insbesondere kritische Infrastrukturen und stark regulierte Sektoren – eng und kontinuierlich in den weiteren Ausgestaltungsprozess einbezogen werden. In diesem Zusammenhang sollten KI und agentische KI-Systeme verhältnismäßig, technisch realistisch und risikobasiert adressiert werden. CADA sollte keine parallelen oder duplizierenden Kontrollregime für Banken und andere regulierte Nutzer schaffen, sondern robuste Nachweis- und Assurance-Mechanismen auf Anbieterebene etablieren, auf die sektorübergreifend vertraut werden kann. Für KI-Dienste sollte dies Transparenz hinsichtlich Datennutzung, Modellbetrieb, Telemetrie, Unterauftragnehmerketten und agentischer Fähigkeiten einschließen, zugleich aber den Zugang zu Innovation erhalten und pauschale Beschränkungen bei der Nutzung leistungsfähiger KI-Dienste vermeiden.

4. Fazit

Das Tech Sovereignty Package und der Cloud & AI Development Act setzen wichtige Impulse zur Stärkung der europäischen digitalen Souveränität und zur Weiterentwicklung eines wettbewerbsfähigen europäischen Cloud- und KI-Ökosystems. Die durch CADA angestoßene Debatte über Eigentum, Kontrolle, Einfluss von Drittstaaten und Lieferketten adressiert zentrale strategische Fragen vor dem Hintergrund zunehmender geopolitischer Fragmentierung.
Die Erfahrungen aus dem Finanzsektor zeigen jedoch, dass digitale Souveränität nicht durch technologische Autarkie oder die pauschale Vermeidung von Abhängigkeiten erreicht wird. Entscheidend ist vielmehr die Fähigkeit, Abhängigkeiten transparent zu machen, Risiken wirksam zu steuern und dauerhafte operative Handlungsfähigkeit in komplexen, global vernetzten IT-Ökosystemen sicherzustellen. Mit DORA verfügt der Finanzsektor über einen etablierten Rahmen für das risikobasierte Management von IKT-Abhängigkeiten, Konzentrationsrisiken, Auslagerungen und Exit-Szenarien. Ein zentrales Strukturprinzip dieses Ansatzes ist die Verlagerung von Nachweis- und Kontrollanforderungen auf IKT-Dienstleister, wodurch redundante Prüf-, Dokumentations- und Governance-Aufwände auf Institutsebene reduziert und Skaleneffekte auf Anbieterseite ermöglicht werden. In der Praxis führt dies zu einer spürbaren Entlastung hoch regulierter Nutzer wie Banken und Sparkassen, ohne die Wirksamkeit des Risikomanagements zu beeinträchtigen. Die daraus gewonnenen Erfahrungen zeigen zugleich, dass Resilienz, Innovationsfähigkeit und digitale Souveränität keine Gegensätze sind, sondern nur im Zusammenspiel wirksam erreicht werden können.
Langfristig wird sich der Erfolg europäischer Souveränitätsambitionen daher nicht daran messen, wo digitale Technologien entwickelt oder betrieben werden, sondern daran, ob es Europa gelingt, technologische Wettbewerbsfähigkeit, Innovationsfähigkeit und eine sichere, selbstbestimmte Nutzung digitaler Technologien in gleichem Maße zu gewährleisten.

Der Bundesverband Öffentlicher Banken Deutschlands, VÖB, ist ein Spitzenverband der deutschen Kreditwirtschaft. Er vertritt die Interessen von 64 Mitgliedern, darunter die Landesbanken sowie die Förderbanken des Bundes und der Länder. Die Mitgliedsinstitute des VÖB haben eine Bilanzsumme von rund 3.100 Milliarden Euro.

Mit einem Marktanteil von über 34 Prozent bei Unternehmenskrediten sind die VÖB-Mitgliedsbanken eine maßgebliche Säule der deutschen Wirtschaft. Sie sind Spitzenreiter bei der Finanzierung der öffentlichen Hand: Ihr Marktanteil bei der Kreditvergabe an Bund, Länder und Gemeinden liegt bei über 66 Prozent.

Die Förderbanken des Bundes und der Länder haben im Jahr 2025 Förderdarlehen in Höhe von knapp 80 Milliarden Euro bereitgestellt. Die VÖB-Institute sind zudem Treiber der nachhaltigen Transformation. Mehr als 50 Prozent des seit 2019 in Deutschland von Banken ausgegebenen Green-Bond-Volumens stammen von VÖB-Mitgliedsbanken.

Die Förderbanken im VÖB haben im Jahr 2025 Förderdarlehen in Höhe von knapp 80 Milliarden Euro bereitgestellt. Als einziger kreditwirtschaftlicher Verband übt der VÖB die Funktion eines Arbeitgeberverbandes für seine Mitgliedsinstitute aus. Die tarifrechtlichen Aufgaben, insbesondere der Abschluss von Tarifverträgen, werden von der Tarifgemeinschaft Öffentlicher Banken wahrgenommen. Ihr gehören 48 Mitgliedsinstitute mit über 65.000 Beschäftigten an.

Weitere Informationen unter www.voeb.de