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

Verordnung über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten (Cybersicherheitsverordnung 2)

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

Kontakt:
Berit Schimm
Telefon: +49 30 2021-2111
Telefax: +49 30 2021-1900
E-Mail: b.schimm@bvr.de

Berlin, 4. Mai 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 „Cybersicherheitsverordnung 2"

Allgemeine Anmerkungen

Aus Sicht der Banken stellt der CSA2 einen Paradigmenwechsel dar: weg von einer primär technisch-operativen Betrachtung hin zu einer stärkeren Einbeziehung geopolitischer Risiken sowie von einem technologieneutralen Ansatz hin zu konkreteren Handlungsvorgaben für die Mitgliedstaaten, etwa im Hinblick auf die Migration zur Post-Quanten-Kryptographie. Diese Entwicklung geht mit strukturellen Unsicherheiten, begrenzter Rechtsklarheit und einer noch nicht abschließend geklärten Rollenverteilung einher.

Im Bankenbereich werden die Cybersicherheits- und IKT-Resilienz-Anforderungen an die Institute über die branchenspezifische DORA-Verordnung formuliert. Für den Finanzsektor gilt die Verordnung (EU) 2022/2554 (DORA) als abschließender, sektorspezifischer Rechtsrahmen für IKT-Risikomanagement, Vorfallsberichterstattung und Drittparteiensteuerung. Der CSA 2-Entwurf als EU-weit geltender, branchenübergreifender Akt wirkt komplementär zu DORA und stellt primär auf das Zusammenwirken mit anderen branchenübergreifenden Akten ab (NIS 2, CRA). Banken sind als wesentliche oder wichtige Unternehmen gemäß Anhang I der NIS 2 qualifiziert. In Bezug auf die NIS 2 gilt DORA jedoch als lex specialis. Dies betrifft insbesondere das Risikomanagement und das Meldewesen der Banken. Besonders deutlich zeigt sich die direkte Überlappung von Verpflichtungen im CRA, etwa durch mögliche parallele Vorfallsmeldungen für denselben Sicherheitsvorfall und redundante Cybersicherheitsbewertungen derselben IT Anwendungen. Zudem deckt DORA das IKT-Drittparteienmanagement umfangreich ab. Die EU sollte in diesem Zusammenhang eindeutig klarstellen, wie die Gesetze zusammenspielen. In jedem Fall sollten die Gesetze so ausgestaltet werden, dass sich keine Doppelregulierung ergibt, d.h. keine zusätzlichen oder parallelen Verpflichtungen für DORA-verpflichtete Institute begründet werden, weder direkt noch indirekt.

Insbesondere sollten etablierte und funktionierende DORA-Strukturen nicht durch horizontale Instrumente ersetzt oder überlagert werden. Eine explizite Klarstellung im Rechtsrahmen ist erforderlich, um Rechtsunsicherheit und Transformationskosten zu vermeiden.

Die NIS 2 war bisher als technologie-neutrale Regulierung angelegt. Mit der gesetzlichen Anforderung an die Mitgliedsstaaten, Richtlinien zur Migration zur Post-Quantenkryptographie zu erlassen, wird dieser Weg verlassen. Zwar ist der Ansatz, die Migration zur Post-Quanten-Kryptographie zu fördern, sicherheitspolitisch nachvollziehbar. Jedoch sollte hier auf bewährte existierende Konzepte aus der NIS-Welt wie "EU Toolbox on ICT Supply Chain Security" zurückgegriffen und diese weiter ausgebaut werden.

Stärkung der Agentur der EU für Cybersicherheit (ENISA)

Die CSA-Revision stärkt ENISA als technische Fachinstanz für Cyberrisiken. Dabei sollte eine klare Zuordnung der Verantwortlichkeiten zwischen ENISA, EBA, EZB und nationalen Aufsichtsbehörden vorgenommen werden. Im Entwurf der CSA 2 ist die Abgrenzung der Zuständigkeiten nicht eindeutig geregelt. Insbesondere ist eine explizite Abgrenzung zu DORA-Audit und Oversight-Mechanismen gegenüber EBA und EZB zwingend erforderlich.

Wir begrüßen, dass die ENISA Warnungen zu Schwachstellen und Vorfällen herausgibt, die aus den CRA- bzw. NIS-2 Meldungen abgeleitet werden. Bei der Bereitstellung von Schwachstelleninformationen sollte ENISA konsequent auf international etablierte Standards, insbesondere das CVE-System, aufsetzen und diese interoperabel nutzen. Europäische Lösungen werden dabei ausdrücklich begrüßt, soweit sie global anschlussfähig sind und auf diesen Standards aufbauen. Andernfalls würden nicht kompatible europäische Parallel- oder Sonderregime die Integration in bestehende Vulnerability-Management-Prozesse der Institute erheblich erschweren. In Bezug auf die Frühwarnungen an wesentlichen oder wichtigen Einrichtungen gemäß

NIS 2 ist bei der Ausgestaltung das Zusammenspiel mit DORA und den zuständigen nationalen Aufsichtsbehörden zu berücksichtigen.

Der CSA 2 greift zudem den bei der ENISA geplanten Single-Entry-Point für das Reporting von Schwachstellen und Vorfällen aus den verschiedenen Gesetzen auf. Ein Single-Entry-Point kann für Unternehmen, die in mehreren Mitgliedstaaten oder nach mehreren Rechtsakten meldepflichtig sind, grundsätzlich Vorteile haben. Gleichzeitig birgt eine zentrale Meldeinfrastruktur erhebliche Risiken und schafft eine neue Abhängigkeit. Fällt diese aus oder weist sie Sicherheitslücken auf, sind sämtliche Meldungen betroffen. Eine zentrale Plattform wird zudem zu einem besonders attraktiven Angriffsziel. Diese Risiken müssen bei der Bewertung des erwartbaren Nutzens angemessen berücksichtigt werden. Vorrangig sollte die inhaltliche Vereinfachung und Vereinheitlichung der Meldeanforderungen selbst verfolgt werden, etwa durch praxisgerechtere Datenfelder und Schwellen, einheitliche Definitionen und abgestimmte Fristen. Erst dadurch würde der CSA 2 dem Finanzsektor einen Vereinfachungsvorteil bieten.

Für den Finanzsektor besteht bereits heute eine weitgehend harmonisierte Vorfallsmeldearchitektur auf Grundlage von DORA. DORA gilt als lex specialis gegenüber NIS2 und CER. Ein verpflichtender oder faktisch ersetzender Single-Entry-Point würde diese bewährten Strukturen aufbrechen, Zuständigkeiten verwischen und erhebliche Umstellungs- und Anpassungskosten verursachen. Für DORA-verpflichtete Institute sollte daher kein zentraler Meldeweg eingeführt werden, der bestehende sektorale Meldeprozesse substituiert. Zu weiteren Details verweisen wir auf unsere Stellungnahme zum Digitalen Omnibus (eingereicht am 10. März 2026 an die Kommission).

Der europäische Zertifizierungsrahmen für die Cybersicherheit

Der CSA 2 stärkt die Rolle von EU-konformen Zertifizierungen u. a. durch die Entwicklung eines Zertifizierungssystems für die „Cyber Posture" von NIS 2 Unternehmen. Wir begrüßen, dass Zertifizierungen zukünftig mit einer Konformitätsvermutung verknüpft werden. Zertifizierungen müssen jedoch freiwillig, risikobasiert und marktorientiert bleiben, da faktische Pflichtzertifizierungen oder zusätzliche Berichtspflichten zusätzliche bürokratische Hürden aufbauen und Investitionen hemmen würden. Art. 71 (4) CSA 2 sieht auch grundsätzlich eine Freiwilligkeit vor, wenn keine anderen Rechtsakte dies bestimmen. Der in Art. 24 (4) NIS 2 Änderung angefügte Absatz, dass Mitgliedstaaten von wesentlichen und wichtigen Einrichtungen verlangen können, ein Zertifikat über die Cyberabwehr zu erlangen, sollte deshalb gestrichen werden.

Ein wirkungsvolles Zertifizierungssystem erfordert allerdings klare Abgrenzungen, ausreichende Kapazitäten und eine enge Verzahnung mit bestehenden Regimen, um der hohen zeitlichen Dynamik und verschiedenen aktuellen Rollen gerecht zu werden.

Die Vorgabe des Art. 82 CSA 2, wonach Konformitätsbewertungen für hohe Vertrauensniveaus grundsätzlich innerhalb des EWR durchzuführen sind, wird kritisch gesehen. Es sollten auch vergleichbare außereuropäische internationale Standards herangezogen können dürfen, Eine strikte geografische Bindung kann zu Engpässen bei Konformitätsbewertungsstellen, Verzögerungen bei sicherheitsrelevanten Updates sowie zu einer Duplizierung global etablierter Test- und Zertifizierungsstrukturen führen.
Zertifizierungen sollten als Konformitätsbeweis für IKT-Dienstleister auch für DORA einsetzbar sein, indem diese auf die Erfüllung der DORA-Anforderungen an Due-Diligence und Steuerung der Dienstleister einzahlen. Keinesfalls sollte aus der Möglichkeit zur Zertifizierung die Pflicht erwachsen, ausschließlich zertifizierte Dienstleister oder Produkte zu nutzen.

Rahmen für vertrauenswürdige IKT-Lieferketten

DORA regelt bereits sehr umfassend die Pflichten von Finanzinstituten/Banken zum IKT-Drittparteienmanagement. Der vom CSA 2 vorgesehene Rahmen ermöglicht u.a. die Auferlegung der Offenlegung der Lieferketten gegenüber den zuständigen Behörden. DORA verfolgt mit dem Informationsregister zu genutzten IKT-Dienstleistungen einen ähnlichen Antritt. DORA-verpflichtete Institute müssen bereits heute ein wirksames IKT-Asset- und Drittparteienmanagement unterhalten und sollten deshalb keinen von DORA abweichenden Pflichten zur Ermittlung von wesentlichen IKT-Assets unterworfen werden (Art. 102 CSA 2).

Maßnahmen nach Art. 103 CSA 2, insbesondere verpflichtende Nutzungsbeschränkungen, die Entfernung von Komponenten oder die Ausphasung sogenannter Hochrisiko-Anbieter, können erhebliche wirtschaftliche und operative Auswirkungen auf Institute haben. Über den Rahmen für IKT-Lieferketten könnten zudem Maßnahmen vorgeschlagen werden, auch wenn keine konkrete nationale Sicherheitsbedrohung aus der jeweiligen Gerichtsbarkeit für die EU besteht. Dies steht im Spannungsverhältnis zu dem in den Erwägungsgründen beschriebenen Ziel des Gesetzes, das primär auf den Schutz vor sicherheitsrelevanten Risiken aus Drittstaaten abstellt. Hinzu kommt, dass unklar bleibt, unter welchen Voraussetzungen Lieferkettenbeschränkungen greifen sollen und wie der zugrunde liegende Prozess konkret ausgestaltet ist, da es bislang an klar formulierten Regelungen und Entwürfen fehlt.

DORA-verpflichtete Institute sollte daher entweder nicht in das CSA-Lieferketten-Rahmenwerk einbezogen werden oder der Umfang zulässiger Risikominderungsmaßnahmen klar begrenzt werden (z.B. keine zusätzlichen Transparenzpflichten). In jedem Fall sind im Rahmen der delegierten Akte - neben angemessenen Übergangsfristen - Härtefallregelungen sowie die Berücksichtigung fehlender marktverfügbarer Alternativen erforderlich. Bei der Bewertung der Verfügbarkeit alternativer Anbieter sind sektorspezifische Marktgegebenheiten (u. a. regulatorische Zulassungen, Hochverfügbarkeit, Sicherheitsanforderungen) zwingend zu berücksichtigen.

Ein rein horizontaler Ansatz ohne sektorale Differenzierung kann - insbesondere für grenzüberschreitend tätige Institute - zu Fragmentierung und erhöhten Risiken führen. Dies zeigt sich auch in der fehlenden Beteiligung der Finanzbehörden an der NIS-Kooperationsgruppe, trotz der erheblichen Bedeutung, die sie bei der Analyse von Lieferketten und der Berücksichtigung geeigneter Minderungsmaßnahmen haben. Finanzbehörden sollten daher in die NIS-Kooperationsgruppe aufgenommen werden, so wie dies die NIS 2 auch grundsätzlich vorsieht.

Fazit

Nur durch eine klare Rollenverteilung, die konsequente Anerkennung sektorspezifischer Regime – insbesondere DORA – sowie eine verhältnismäßige Ausgestaltung exekutiver Eingriffsbefugnisse lassen sich die Ziele von CSA 2 erreichen, ohne Stabilität, Innovationsfähigkeit und Wettbewerbsfähigkeit des europäischen Finanzsektors zu beeinträchtigen.