bankenverband

Stellungnahme

des Bankenverbandes
„Zehn Punkte für ein modernes Drittparteien-Risikomanagement“

11. Juni 2025

Lobbyregister-Nr. R001458
EU-Transparenzregister-Nr. 0764199368-97

Diana Campar
Associate Director
Telefon: +49 30 1663-1546
diana.campar@bdb.de

Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin
Telefon: +49 30 1663-0
Website: bankenverband.de

USt.-IdNr. DE201591882

Zehn Punkte für ein modernes Drittparteien-Risikomanagement

Die zunehmende Digitalisierung und das Nutzen von Wertschöpfungsketten im Finanzsektor verlangen eine grundlegende Neuausrichtung der regulatorischen Rahmenbedingungen für das Management des Drittparteienrisikos. Vor dem Hintergrund des neuen europäischen Digital Operational Resilience Act (DORA), der seit dem 17. Januar 2025 angewendet wird, und der anstehenden Überarbeitung der Leitlinien zu Auslagerungen der Europäischen Bankenaufsicht (EBA) spricht sich der Bankenverband für ein konsistentes, international anschlussfähiges und zukunftsgerichtetes Regelwerk aus.

Von der Auslagerung zum Third-Party Risk: Paradigmenwechsel notwendig

Die bestehende Auslagerungsregulierung ist noch vor Beginn der digitalen Transformation des Bankgeschäfts entstanden. Seitdem ist viel passiert: Banken sind heute in ein Netzwerk unterschiedlichster Drittparteienbeziehungen eingebunden – von klassischen Dienstleistern über Cloud-Anbieter bis hin zu globalen Technologiepartnern. Entscheidend ist dabei nicht mehr die rechtliche Schublade, in die eine Beziehung fällt, sondern das Risiko, das aus der Beziehung entsteht.
Ein zukunftsfähiger regulatorischer Ansatz sollte daher vollständig risikobasiert, ergebnisorientiert und technologieoffen sein. Die Einordnung von Drittparteien in Kategorien wie „Auslagerung", „IKT-Dienstleistung" oder „sonstiger Fremdbezug" sollte perspektivisch entfallen. Stattdessen ist ein einheitliches Modell erforderlich, das den Risikograd einer Aktivität bzw. Funktion allein aus der Bedeutung der institutsspezifischen Prozesse ableitet – unabhängig von Begrifflichkeiten der Vergangenheit.

Harmonisierung mit DORA: Keine zusätzlichen Anforderungen

DORA setzt einen neuen europäischen Standard für den Umgang mit IKT-bezogenen Drittparteien. Die EBA-Leitlinien zu Auslagerungen, die demnächst überarbeitet werden, sollten sich eng daran orientieren und keine darüberhinausgehenden Anforderungen formulieren. Das Prinzip der vorrangigen Anwendung von DORA bei IKT-bezogenen Dienstleistungen gilt es beizubehalten. Die EBA-Leitlinien sollen nur für die nicht IKT-bezogenen Leistungen Anwendung finden, jedoch keine zusätzlichen Belastungen hervorrufen.
Insbesondere bei vertraglichen Mindestinhalten, Registerführung, Due Diligence und Ausstiegsstrategien darf es keine regulatorische Doppelspur geben. Ein konsistentes Rahmenwerk ist nicht nur eine Frage der Effizienz, sondern der Rechtssicherheit und der praktischen Umsetzbarkeit.

Für eine echte Harmonisierung ist auch eine gemeinsame Sichtweise der europäischen Aufsichtsbehörden entscheidend. Nationale Besonderheiten in der Aufsichtspraxis können trotz weitgehender Angleichungen zu erheblichem Mehraufwand führen – insbesondere für grenzüberschreitend tätige Institute. Eine Fragmentierung bindet unnötig Ressourcen, die für das effektive Management realer operationeller Risiken eingesetzt werden sollten. Regelwerke sollten daher nicht nur formal aufeinander abgestimmt sein, sondern auch in der praktischen Anwendung einheitlich interpretiert und umgesetzt werden – im Einklang mit der EU-Agenda für Wettbewerbsfähigkeit und der erklärten politischen Absicht, regulatorische Anforderungen zu vereinfachen und praktikabler zu gestalten.

Proportionalität: Der Schlüssel für praktikable Regulierung

Die künftigen EBA-Vorgaben dürfen Institute nicht durch übermäßige Komplexität belasten – insbesondere kleine und sehr kleine Institute brauchen ausreichend Spielraum bei der Umsetzung. Eine praxisnahe, proportionale Ausgestaltung ist entscheidend, um die unterschiedlichen Strukturen und Ressourcen realistisch zu berücksichtigen. Statt detaillierter Einzelvorgaben sollte eine prinzipienbasierte Regulierung im Vordergrund stehen. Nur so lassen sich Flexibilität, Umsetzbarkeit und ein angemessenes Maß an Aufsicht miteinander in Einklang bringen – ohne die Institute zu überfordern.
Die Auslagerungsvorgaben müssen an die unmittelbar und vorrangig geltenden DORA-Regeln, die eine Berücksichtigung von Größe, Risikostruktur und Komplexität bei der Umsetzung vorschreiben, angepasst und durch konkrete Regelungen weiter präzisiert werden.
Ein abgestuftes, risikoorientiertes Umsetzungsmodell mit Erleichterungen für kleinere Institute kann etwa durch standardisierte Vertragsbausteine, reduzierte Prüfanforderungen und den Verzicht auf komplexe Tests sichergestellt werden. Proportionalität muss dabei verbindlich und systematisch dokumentiert, durch Governance-Prozesse begleitet und überprüfbar sein. Für kleinere Institute sind daher klare Schwellenwerte und standardisierte Verfahren im Einklang mit den Schutzzielen der Aufsicht notwendig.

Einheitliche Definition kritischer Funktionen: Klarheit und Konsistenz schaffen

Die Feststellung, ob eine Drittparteienbeziehung eine kritische oder wesentliche Funktion unterstützt, ist ein zentraler Baustein eines verhältnismäßigen und risikobasierten Ansatzes für das Risikomanagement. Die Definitionen in den verschiedenen Regelwerken divergieren jedoch. Diese Abweichungen führen zu Unsicherheiten, unnötiger Komplexität und Inkonsistenzen in der Praxis.
Wir fordern daher eine Harmonisierung der Kritikalitätsbestimmung – sowohl im Grundsatz als auch in den operativen Auswirkungen (z. B. Registerführung, Vertragsinhalte, Steuerungsmaßnahmen). Die Feststellung der Kritikalität sollte dabei stets prozessorientiert erfolgen und nicht durch nachgelagerte Risikoanalysen ausgeweitet werden. Die Auslagerung von

Aktivitäten und Prozessen, die nicht als kritisch gelten, kann per se nicht wesentlich sein. Die mit einer Auslagerung verbundene Risikoerhebung dient dem Zweck, eine risikoadäquate Steuerung sicherzustellen und diese zu überwachen. Sie ist daher von der Kritikalitätsbestimmung abzugrenzen.

Global denken, praktikabel handeln: Vermeidung regulatorischer Fragmentierung

Für international tätige Institute stellen unterschiedliche nationale und regionale Anforderungen einen erheblichen Umsetzungsaufwand dar. Globale Prozesse und zentrale IT-Systeme lassen sich nur mit hohem manuellem Aufwand an nationale Sonderregelungen anpassen – dies konterkariert Effizienz und Effektivität im Risikomanagement.
Harmonisierung darf nicht an der EU-Grenze enden, deshalb sollte ein einheitlicher europäischer Ansatz auch die Anschlussfähigkeit an internationale Regelwerke und Standards berücksichtigen. Die EU-Vorschriften sollten mit Blick auf die globale Interoperabilität entwickelt und so verhältnismäßig sein, dass sie die Wettbewerbsfähigkeit und die operative Widerstandsfähigkeit von grenzüberschreitend tätigen Unternehmen unterstützen.

Konzerninterne Dienstleister: Risikoorientierung statt Gleichbehandlung

Besondere Erleichterungen sind für konzerninterne Drittparteienbeziehungen erforderlich. Eine Servicegesellschaft innerhalb des Konzerns lässt sich anders steuern als ein externer Dienstleister. Hier ist Augenmaß gefragt – kein vollständiger Verzicht auf Steuerung, aber eine risikoorientierte Differenzierung.
Auch Leistungsbeziehungen innerhalb einer juristischen Einheit – z. B. zwischen Zentrale und Auslandseinheiten – dürfen nicht als Drittparteienverhältnis eingestuft werden, da sie strukturell keine externe Leistungserbringung darstellen.

Unterauftragnehmer und Weiterverlagerungen: Proportionalität sicherstellen

DORA geht beim Thema Unterauftragsvergabe sehr in die Tiefe – oft zu tief. Eine Übertragung dieser Anforderungen auf nicht-IKT-bezogene Beziehungen ist daher nicht zielführend. Erforderlich ist ein risikoorientiertes Maß an Transparenz und Steuerung, aber kein generelles Misstrauensprinzip. Die Erwartungen der Regulierungs- und Aufsichtsbehörden sollten vielmehr auf einem praktikablen und risikobasierten Ansatz beruhen, der sich auf „wichtige" oder „wesentliche" Unterauftragnehmer konzentriert.
Die Wesentlichkeit von Weiterverlagerungen sollte ausschließlich aus der Bedeutung der unterstützten Funktion abgeleitet werden und insbesondere jene Unterauftragnehmer fokussieren, die eine wesentliche Rolle bei der Unterstützung einer kritischen oder wichtigen

Funktion spielen, deren Störung die Erbringung der Dienstleistung wesentlich beeinträchtigen könnte.

Praxistauglichkeit im Fokus: Umgang mit spezialisierten Dienstleistern

Regulatorische Vorgaben müssen so ausgestaltet sein, dass sie auch in der Zusammenarbeit mit spezialisierten Nischenanbietern umsetzbar bleiben. Solche Dienstleister bewegen sich in der Regel außerhalb des klassischen regulatorischen Rahmens. Hier stoßen viele Banken an strukturelle Grenzen, insbesondere wenn Anforderungen zu Vertrags- und Berichtspflichten praktisch nur schwer erfüllbar sind. Auch bei den IT-Leistungen innerhalb bankeigener Infrastrukturen entstehen Interpretationsspielräume, die regulatorisch klarer eingeordnet werden sollten. Die aufsichtsrechtlichen Rahmenbedingungen müssen diesen Realitäten Rechnung tragen und praktikable Lösungen ermöglichen – insbesondere für kleinere und mittelgroße Institute.

Nicht alles ist relevant: Klare Abgrenzung und Whitelist erforderlich

Ein effektives Drittparteien-Risikomanagement erfordert Klarheit darüber, was nicht in den Anwendungsbereich fällt. Dazu zählen z. B. Lieferanten für Büromaterial, einfache Facility-Services oder bereits beaufsichtigte Unternehmen. Regulierte Dienstleistungen, die von beaufsichtigten Finanzunternehmen erbracht werden, sollten nicht unter die Regularien fallen, da dies zu einer unzweckmäßigen Doppelregulierung führt.
Eine klare Negativliste (Whitelist) muss Bestandteil der Regulierung sein. Sonderfälle wie Kooperationen, Joint Ventures oder Sponsoringvereinbarungen müssen gesondert betrachtet werden – hier besteht keine unmittelbare Leistungs- oder Datenbeziehung.

Ein Register – ein System: Einheitliche und schlanke Umsetzung

Die Anforderungen an Register und Berichterstattung dürfen nicht zu einem doppelten Verwaltungsakt führen. Die Registerstruktur gemäß DORA-ITS sollte auch für Nicht-IKT-Drittparteien übernommen werden – bei gleichzeitigem Wegfall nicht relevanter Felder (z. B. Cloud-Modell oder Entscheidungsgremium). Es braucht eine zentrale, harmonisierte Erfassung – sowohl bei den Instituten als auch für die Aufsicht, einschließlich eines einheitlichen Umsetzungsprozesses hinsichtlich des Stichtags und der Einreichungsdaten sowie deren Validierung. Nationale Unterschiede bei der Umsetzung des Registers führen zu erheblichen operativen Problemen in der gesamten Branche und Herausforderungen bei der Einhaltung der Fristen für die Einreichung.
Auch die Informationen und Vertragsbestandteile sollten im Verhältnis zum Risiko stehen, zum Beispiel durch Abstufung der Anforderungen abhängig vom Risikograd der Dienstleistung, um eine ungerechtfertigte Ressourcenbindung zu vermeiden.

Fazit: Die Zukunft ist Third-Party Risk – nicht Auslagerung

Die digitale Transformation verlangt einen Paradigmenwechsel: weg von der überholten Vorstellung der Auslagerung als Sonderfall, hin zu einem ganzheitlichen Third-Party-Risk-Modell. Die Überarbeitung der EBA-Leitlinien ist eine Chance, diesen Wandel regulatorisch zu vollziehen. Konsistenz, Proportionalität und internationale Anschlussfähigkeit müssen die Leitplanken sein. Nur so lassen sich Risiken effektiv steuern – und gleichzeitig Innovation und Wettbewerbsfähigkeit im europäischen Finanzsektor sichern.