Foto: Glenn Carstens Peters, Unsplash

BVR-Positionen Nr. 8/ Januar 2021

Cyberresilienz effizient gestalten – DORA Vorschlag anpassen

BVR-Positionen zum Digital Operational Resilience Act (DORA)
der Europäischen Kommission

Bundesverband
der Deutschen Volksbanken
und Raiffeisenbanken · BVR

Bundesverband
der Deutschen Volksbanken
und Raiffeisenbanken · BVR

Vorwort

Chancen der Digitalisierung nutzen, Risiken eindämmen

Das Zeitalter der Digitalisierung hat durch die aktuelle COVID-Pandemie einen kräftigen Impetus erhalten. Die Nutzung neuer Technologien eröffnet große Chancen im Bereich innovativer Finanzdienstleistungen, begründet aber auch große Herausforderungen. Die Cybersicherheit ist eine davon, und so ist das Ziel der Europäischen Kommission richtig gesetzt, alle Teilnehmer des Finanzsystems zu notwendigen Sicherheitsvorkehrungen zu verpflichten, um Cyber-Angriffe und andere IKT-Risiken einzudämmen.

Die Europäische Kommission hat folgerichtig im September 2020 im Rahmen ihres *Digital Finance Package* einen umfangreichen Verordnungsvorschlag zum Thema *Digital Operational Resilience* im Finanzsektor (kurz DORA) vorgelegt, welcher Anforderungen im Bereich der Cyberresilienz an alle Teilnehmer des Finanzsystems stellt. Zugleich hat sie ein Rahmenwerk zur Beaufsichtigung von kritischen Drittanbietern von Informations- und Kommunikationstechnologien (IKT) für Finanzunternehmen erarbeitet.

Der BVR begrüßt die Harmonisierung der bestehenden Regeln im Bereich der Cybersicherheit ausdrücklich, denn sie ist mit Blick auf die Fraktionierung der aktuellen Vorschriften überaus wünschenswert.

Dabei ist jedoch auf eine gute Balance zu achten: Die neuen Regelungen sollen die Arbeit der Kreditinstitute nicht unnötig erschweren und keinesfalls zu einer geringeren Effizienz bei der Umsetzung der Maßnahmen zur Informationssicherheit führen.

Der aktuelle DORA-Vorschlag geht jedoch weit über den von der Europäischen Kommission beabsichtigten Ansatz der Harmonisierung hinaus. Zudem bietet die vorgeschlagene Verordnung im Gegensatz zu den bisher geltenden Leitlinien keine Möglichkeiten der Berücksichtigung nationaler Besonderheiten und auch das so wichtige Prinzip der Proportionalität wird nicht ausreichend berücksichtigt.

Insbesondere im IT-Sicherheitsumfeld muss die kurzfristige Anpassungsfähigkeit der Methoden und Praktiken sichergestellt werden, um ein effizientes Handeln bei sich ändernden Bedingungen zu gewährleisten.

In diesem Papier führen wir die BVR-Petiten für eine effiziente regulatorische Gestaltung der Cybersicherheit im Finanzsektor auf.

Marija Kolak
Präsidentin

Gerhard Hofmann
Mitglied des Vorstands

Dr. Andreas Martin
Mitglied des Vorstands

Bundesverband
der Deutschen Volksbanken
und Raiffeisenbanken · BVR

Cyberresilienz effizient gestalten

1. Proportionalität wahren und prinzipienorientiert vorgehen

DORA ist ein wichtiger Schritt zur weiteren Harmonisierung des europäischen digitalen Binnenmarktes. Der BVR begrüßte die Intention und die grundsätzliche Vorgehensweise der Kommission ausdrücklich, er fordert jedoch zugleich, dass das so wichtige Prinzip der Proportionalität Eingang in DORA findet.

Insbesondere für kleinere Finanzinstitute sind die vorgeschlagenen Anforderungen teilweise zu weitgehend. So werden der Geschäftsleitung zu viele Aufgaben direkt zugeordnet, ohne dass eine risikoorientierte Auslegung der Regelungen ermöglicht wird. Zwar enthält der Kommissionsvorschlag gewisse Ausnahmeregelungen für sogenannte „Micro-enterprises", diese lassen sich aber nicht im deutschen Bankenmarkt nutzen, denn selbst sehr kleine Volks- und Raiffeisenbanken fallen nicht unter die Definition.

Die aktuellen Vorschläge der Kommission beinhalten viele Einzelregelungen, die an Stelle der aktuell gültigen prinzipienorientierten Vorgaben treten sollen. Anders als bei den bisher geltenden EBA-Leitlinien bietet die Verordnung keinen Raum, um nationale Besonderheiten zu berücksichtigen.

Über die vorgesehenen Regulatory Technical Standards (RTS) der Europäischen Aufsichtsbehörden (ESAs) ist zudem eine noch weitergehende Regelungsdichte zu erwarten. Der BVR spricht sich gegen eine solche regulatorische Methodenfestlegung in zahlreichen Details über RTS aus, da im IT-Sicherheitsumfeld eine kurzfristige Anpassungsfähigkeit der Methoden und Praktiken bei sich ändernden Gefahrenlagen erforderlich ist.

Detailliertere Anforderungen sollten deshalb weiterhin in Form von EBA-Leitlinien formuliert werden, um eine risikoorientierte Auslegung der prinzipienorientierten Anforderungen zu ermöglichen und nationale Besonderheiten berücksichtigen zu können.

2. Harmonisierung des Meldewesens positiv

Der BVR unterstützt die von der Europäischen Kommission angedachte Harmonisierung des Meldewesens bei Sicherheitsvorfällen. Insbesondere mit Blick auf die Fraktionierung der aktuellen Vorschriften ist diese überaus wünschenswert, denn sie ermöglicht es, die unterschiedlichen Meldevorschriften und Templates zu vereinheitlichen und somit die Verfahren bei Sicherheitsvorfällen zu vereinfachen.

Dabei ist allerdings darauf zu achten, dass die neuen Regelungen keinen administrativen Zusatzaufwand auslösen, der die Effizienz der Finanzinstitute bei der Bearbeitung von Sicherheitsvorfällen letztlich sogar beeinträchtigen und sich somit negativ auf die Cybersicherheit der Institute auswirken würde.

Deshalb sollten die bestehenden Anforderungen an ein Vorfallreporting u.a. aus der PSD2 und der NIS-Richtlinie durch das neue Reporting vollständig abgedeckt werden, damit in Zukunft nur noch ein zentrales Meldeformular über einen Meldeweg eingereicht werden muss.

3. Erleichterungen für Verbünde bei IT-Auslagerung

Die Europäische Kommission sieht in ihrem Verordnungsvorschlag vor, dass Finanzunternehmen im Rahmen ihres Risikomanagements verpflichtet werden sollen, Konzentrationsrisiken besonders zu berücksichtigen, die u.a. durch die Nutzung eines IT-Dienstleisters für mehrere Services entstehen können. Auch wenn die vorgeschlagene Strategie keine verpflichtende Nutzung mehrerer IKT-Dienstleister bedeutet, so sind die damit verbundenen Dokumentationspflichten bei Auslagerung auf Verbunddienstleister nicht erforderlich und sollten daher in der Endfassung von DORA nicht mehr enthalten sein.

Die Banken der genossenschaftlichen Finanzgruppe haben die Entwicklung und den Betrieb der IT an einen zentralen IT-Dienstleister (Fiducia & GAD IT AG) ausgelagert, der im Eigentum der angeschlossenen Banken ist, sodass diese ihre Anforderungen über standard-vertragliche Formen hinausgehend wirksam geltend machen können. Eine solche Auslagerung innerhalb eines Finanzverbundes ermöglicht eine Risikominderung durch die Erhöhung der

technischen Professionalität und darf deshalb nicht mit erhöhtem administrativen Aufwand belastet werden.

Die Genossenschaftsbanken gehören zudem einem institutsbezogenen Sicherungssystem an, in dessen Rahmen präventive Maßnahmen zur Abwendung von Fehlentwicklungen bei den einbezogenen Instituten ergriffen werden. Darüber hinaus wurde ein zentrales Auslagerungsmanagement eingerichtet, das die Institute bei der Überwachung des zentralen IT-Dienstleisters fachlich unterstützt.

In den MaRisk werden auf Basis der EBA-Leitlinien zum Outsourcing Erleichterungen für IT-Auslagerungen auf Gruppen- bzw. Verbundebene festgelegt:

- Risikomindernde Berücksichtigung eines einheitlichen und umfassenden Risikomanagements bei der Erstellung und Anpassung der Risikoanalyse
- Einrichtung eines zentralen Auslagerungsmanagements
- Verzicht auf Erstellung von Ausstiegsprozessen und Handlungsoptionen

Diese Regelungen finden in den neuen Vorschlägen zu DORA allerdings keine Berücksichtigung mehr.

Der BVR spricht sich explizit für eine Aufnahme dieser Erleichterungen aus, da damit den wirksam getroffenen Vorkehrungen auf Ebene der genossenschaftlichen FinanzGruppe Rechnung getragen wird und somit administrative Aufwände auf Ebene der einzelnen Bank reduziert werden können.

4. Anforderungen an das Management von IKT-Drittdiensten risikoorientiert abstufen

Bei den Anforderungen an das Management von IKT-Drittdiensten sollte unterschieden werden, ob die IKT kritische bzw. wesentliche Funktionen unterstützen oder lediglich nachgelagerte Funktionen. Die vertragliche Einräumung von Zugangs- und Prüfrechten sowie die Zusammenarbeit mit den Aufsichtsbehörden sollte im Einklang mit dem risikobasierten Ansatz bei der Ausübung der Zugangs- und Prüfungsrechte in Bezug auf den IKT-Drittanbieter erfolgen. Eine vertragliche Vereinbarung sollte nur bei IKT-Services, die kritische bzw. wesentliche Funktionen unterstützen, vorgeschrieben werden. Da die Standardverträge von IKT-Drittanbietern solche Prüfrechte in der Regel nicht vorsehen, wären ansonsten für alle Services zusätzliche Vereinbarungen zu treffen, was die Nutzung solcher Services erschwert oder sogar verhindert und einen erheblichen Zusatzaufwand verursacht.

Die Bestimmungen zur Vertragsbeendigung scheinen absolut zu sein und gehen über die Anforderungen der derzeit umgesetzten EBA-Leitlinien hinaus. Insbesondere die Anforderungen an Finanzinstitute, Vertragsbeziehungen im Falle von Vertragsbrüchen - ohne jegliche Wesentlichkeitsgrenze - zu beenden, stellt einen unverhältnismäßigen Eingriff in die Vertragsfreiheit dar.

5. Aufsichtsrahmen für kritische IKT-Drittanbieter vor allem auf Hyperscaler ausrichten

Wir begrüßen die Idee eines neuen Aufsichtsrahmens für kritische europaweit tätige IKT-Drittanbieter. Dieser sollte auf international tätige Dienstleister ausgerichtet werden, bei denen die Durchsetzbarkeit von Prüfungen auf der Ebene des einzelnen Finanzinstituts nicht ausreichend gewährleistet werden kann (sogenannte Hyperscaler).

Der Aufsichtsrahmen für kritische IKT-Drittanbieter sollte mit Erleichterungen im Hinblick auf eigene Prüfungshandlungen für auslagernde Finanzinstitute verknüpft werden, da diese Anbieter direkt beaufsichtigt werden.

Für national tätige IKT-Dienstleister sollte eine Prüfung allerdings weiterhin durch nationale Aufsichtsbehörden erfolgen, da diese die nationalen Gegebenheiten genauestens kennen.

Die Aufforderung durch Aufsichtsbehörden, Verträge zwischen Finanzinstituten und kritischen IKT-Dienstleistern zu suspendieren oder gar zu beenden, kann nur das letzte Mittel sein und erfordert eine enge vorausgehende Abstimmung mit den betroffenen Finanzinstituten. Bevor es zu einer derartigen Eskalation kommt, sollte geprüft werden, inwiefern das Ziel durch Risikoreduzierungsmaßnahmen erreicht werden kann. Ein Wechsel des IKT-Dienstleisters benötigt in jedem Fall einen ausreichenden zeitlichen Vorlauf für das Finanzinstitut.

6. Ausreichende Umsetzungsfristen

Schließlich ist darauf zu achten, dass dem Markt genügend Zeit für die Umsetzung der neuen Regelungen eingeräumt wird. Dies ist auch mit Blick auf die geplanten Regulatory Technical Standards von großer Bedeutung, denn die Detailregelungen werden erst nach Annahme des Legislativvorschlags erarbeitet und sind somit erst zu einem sehr späten Zeitpunkt verfügbar.

Da die Umsetzung neuer Anforderungen durch die Finanzinstitute einen zeitlichen Vorlauf benötigen, spricht sich der BVR für eine Verlängerung der Umsetzungsfristen von 12 auf 36 Monate aus.

- Die Harmonisierung im Meldewesen ist ein guter Schritt. Wichtig ist, dass die bestehenden Anforderungen an ein Vorfallreporting u.a. aus der PSD2 und der NIS-Richtlinie durch das neue Reporting vollständig abgedeckt werden.
- Der Schwerpunkt eines neuen Aufsichtsrahmens für kritische IKT-Dienstleister sollte vor allem auf (international tätige) Hyperscaler ausgerichtet werden.
- Die Prüfung national tätiger IKT-Dienstleister sollte weiterhin durch nationale Aufsichtsbehörden erfolgen.
- Der Aufsichtsrahmen für kritische IKT-Dienstleister sollte mit Erleichterungen bei der Überwachung durch auslagernde Finanzinstitute verknüpft werden.
- Der BVR spricht sich für eine Verlängerung der Umsetzungsfristen von 12 auf 36 Monate aus.

Petiten des BVR

- Der BVR begrüßt den Harmonisierungsansatz im Bereich der Cyberresilience. Die aktuellen Vorschläge der EU-Kommission gehen aber weit darüber hinaus.
- Eine risikoorientierte Auslegung der Anforderungen unter Berücksichtigung nationaler Besonderheiten muss ermöglicht werden. Der BVR spricht sich deshalb dafür aus, detaillierte Anforderungen weiterhin in Form von EBA-Leitlinien anstelle von RTS zu formulieren, da im IT-Sicherheitsumfeld eine kurzfristige Anpassungsfähigkeit zwingend erforderlich ist.
- Erleichterungen für IT-Auslagerungen auf Gruppen- bzw. Verbundebene, wie sie durch die MaRisk auf Basis der EBA-Leitlinien zum Outsourcing vorgesehen sind, haben sich bewährt und sind weiterhin erforderlich.
- Die enthaltenen Ausnahmeregelungen für sogenannte „Micro-enterprises" lassen sich nicht nutzen, denn selbst sehr kleine Genossenschaftsbanken fallen nicht unter die Definition. Insbesondere kleinen und nicht komplexen Instituten sollten Ausnahmen ermöglicht werden.

ANSPRECHPARTNER:

Berit Schimm, zuständige Fachabteilung Berlin (b.schimm@bvr.de)
Selina Glaap, Politische Interessenvertretung in Brüssel (s.glaap@bvr.de)

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken • BVR
Verbindungsstelle Parlament/ Europapolitik
Schellingstraße 4, 10785 Berlin
Kontakt: Thomas Stammen, Mirian Fabian Breuer, Selina Glaap, Dr. Volker Heegemann und Julia Weishaupt
Telefon: +49 30 2021 1605, Mail: politik@bvr.de, Internet: www.bvr.de

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR)

Der BVR ist der Spitzenverband der genossenschaftlichen Kreditwirtschaft in Deutschland. Dazu zählen die 841 Volksbanken und Raiffeisenbanken, Sparda-Banken, PSD Banken, Kirchenbanken und weitere Sonderinstitute wie die Deutsche Apotheker- und Ärztebank. Präsidentin des BVR ist Frau Marija Kolak. Weitere Mitglieder des Vorstandes sind Gerhard Hofmann und Dr. Andreas Martin. Der BVR vertritt bundesweit und international die Interessen der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken. Innerhalb der Gruppe koordiniert und entwickelt der BVR die gemeinsame Strategie der Volksbanken und Raiffeisenbanken.

Er berät und unterstützt seine Mitglieder in rechtlichen, steuerlichen und betriebswirtschaftlichen Fragen. Der BVR betreibt ferner zwei institutsbezogene Sicherungssysteme. Dies ist zum einen die 100-prozentige Tochtergesellschaft „BVR Institutssicherung GmbH", welche das amtlich anerkannte Einlagensicherungssystem darstellt, und zum anderen die freiwillige „Sicherungseinrichtung des BVR" – das älteste Bankensicherungssystem Deutschlands. Der BVR ist aktiv in Berlin, Bonn und Brüssel. Informationen zum BVR und seinen Themen erhalten Sie über: politik@bvr.de oder unter +49 (0)30 2021 1605 oder auf der Website www.bvr.de.